

## **Biometrie - Bequemlichkeit und Sicherheit kombiniert?**

By Elmar Hilgers, Managing Director & Co-founder, IdentAlink Ltd.  
November 12, 2003

Es ist Montagmorgen. Sie sind soeben – nach einem 2-wöchigen Urlaub am Strand - im Büro angekommen. Der morgendliche Verkehr war mal wieder grauhaft und Sie hatten auch noch vergessen den Wecker zu stellen. Das Letzte wo Ihnen jetzt der Sinn nach steht ist ARBEIT. Hört sich das bekannt an? Sie kommen zu Ihrem Schreibtisch. Sie schalten Ihren Computer an. Und dann, Stopp. Wie war noch mal das letzte Passwort welches Sie beim IT Support registriert hatten?

Im ersten Versuch schreiben Sie den Namen Ihrer Lebensgefährtin. ZUGANG VERWEIGERT! Sie schreiben den Namen Ihres Hundes. ZUGANG VERWEIGERT! Schon leicht verärgert tippen Sie den Namen Ihres Sohnes ein. ZUGANG VERWEIGERT! Sie tippen die letzten vier Zahlen Ihrer Telefonnummer ein. IMMER NOCH KEIN ZUGANG! Sie schauen sich überlegend das Bild Ihres Lieblingsteams auf dem Schreibtisch an und schreiben zögernd H-E-R-T-H-A-B-S-C.

An diesem Punkt hat Sie Ihr Netzwerk mit Sicherheit schon als potentiellen Eindringling erkannt und den Zugang zu Ihrem Computer total gesperrt. Mit einem tiefen Seufzer greifen Sie nach dem Telefon und rufen den IT Support. Ihre Anfrage steht nun im Log aber bis einer vom IT Department kommt oder Ihnen Ihr neues Passwort mitteilt bleibt Ihnen nicht viel mehr übrig als „die Daumen zu rollen“.

Umsomehr elektronische Prozesse im Geschäftsleben übernommen werden, desto höher werden die Anforderungen an Sicherheit in allen Belangen des täglichen Lebens (physische Zugangskontrollen für das Heim, Büros, Banken etc.), hier können wir alle schon die Grenzen von Passwörtern und PIN Nummern selbst erfahren. OK, wir könnten einige der PINs ändern damit wir uns nicht sooo viele zu merken haben. Aber versuchen Sie sich mal den PIN für die Einbruchssicherung Ihres Hauses, das Codewort für Ihr Internet Online banking, den PIN von Ihrer Bankcard für den Geldautomaten, den PIN für Ihre Visakarte und das Passwort für den Zugang zum Firmennetzwerk zu merken. Und das ist nur das halbe Problem. Wenn Sie Ihren Code oder Passwort sich einfach merken wollen, müssen Sie sich etwas aussuchen was sich einfach in Ihrem Gehirn einbrennt.

Deshalb ist es keine Überraschung das Geburtstage, Haustiernamen, Kindernamen oder der Name Ihres Lieblingsteams ausgesucht werden. Und hier kommt das nächste Problem: Die Tatsache das sehr viele Menschen solche Hilfestellungen für Ihren Code oder Passwort nutzen, macht es sehr einfach für einen potentiellen Kriminellen erfolgreich die Passwörter zu erraten/erfragen.

Wie viele Arbeitsstunden gehen verloren weil Mitarbeiter Ihre Passwörter vergessen? Und wie viel Kosten entstehen um Passwörter monatlich zu ändern bzw. neu zu Verfügung zu stellen?

Glaubt man Angaben aus der Industrie, veröffentlicht von seriösen Unternehmen wie der Gartner Group, dann belaufen sich die Kosten der Administration in einem mittleren Netzwerk mit ca. 200 Anwendern auf ca. EURO 280 pro Jahr pro Anwender. Bei solch hohen Kosten ist es nicht überraschend das vielen Firmen und Organisationen nach alternativen Sicherheitsmöglichkeiten suchen. Eine Alternative könnte die Nutzung von Smartcards oder Schlüssel sein.

Aber diese haben eine anhaftende Schwäche: Welche Methoden sind dann notwendig um sicherzustellen das die Person welche sich Zutritt verschafft auch die ist welche Sie vorgibt zu sein? Und was passiert wenn ich meine Smartcard oder Schlüssel verliere? Es könnte Tage dauern, oder sogar Wochen um Ersatz zu beschaffen.

Ein anderer Weg wäre die Nutzung von biometrischen Technologien. Die Biometrie ersetzt etwas was wir wissen (z.B. Passwörter oder PINs), oder etwas was wir besitzen (z.B. Smartcards oder Token), mit etwas Einzigartigem von uns (einer physischen Charakteristik wie z.B. das Gesicht, Fingerprint, Signatur, Stimme oder Iris). Anders als bei Passwörtern, Smartcards und Tokens, hat die Biometrie den Vorteil dass man sie nur sehr schwer nachahmen kann, duplizieren oder stehlen kann.

Diese Technologie ist schon seit Jahren auf dem internationalen Markt bekannt. Wie auch immer, erst in den letzten vier bis fünf Jahren konnte man einen Zuwachs in den Anwendungen verfolgen. Fallende Hardware Preise kombiniert mit erhöhtem Bedarf für sichere Authentifikation, mit der Möglichkeit eines Audits per Anwender, haben das Interesse auf beiden Seiten des Atlantiks steigen lassen.

Biometrie wird im Moment für eine Reihe von Applikationen genutzt inklusive Einwanderungsbehörden, Zugangskontrolle in Banken, Gefängnisse und Atomkraftwerken. Im unteren Sicherheitssegment des Marktes bietet Biometrie Bequemlichkeit gepaart mit zusätzlicher Sicherheit für Sozialhilfeauszahlungen, Krankenkassen und im Computer Sicherheitsmarkt. Man höre und staune, sogar Schulkinder nutzen die Technologie in Schulkantinen oder Büchereien.

Als bald die Biometrie mehr und mehr in den Vordergrund rückte, überraschend viele "Spezialisten" melden sich zu Wort um Mythen unter die Leute zu bringen. Speziell Themen wie Privatsphäre, Datensicherheit und allgemeine Schwächen haben den Weg in die Schlagzeilen geschafft, sehr oft mit inakkuraten und unvollkommenen Geschichten. Niemand in der Biometrie Gemeinde behauptet das die Technologie 100% sicher ist. Wie auch immer, die Biometrieindustrie versucht die kosten effektivste und doch sicherste und bequemlichste Alternative zu traditionellen Formen der Identifikation und Verifikation zu bieten.

Einige Fingerprintlesegeräte (Sensoren) bieten Grund zur Sorge und wurden deswegen schon vom Markt entfernt, aber die Hardwareindustrie ist steht's bemüht die entsprechenden Lesegeräte auf einen Stand zu bringen der den neuesten kriminellen Techniken widersteht. Man sollte aber nie vergessen dass mit genügend krimineller Energie und Zeit es möglich sein könnte auch das sicherste Gerät zu überwinden.

Wir müssen lediglich sicherstellen dass der Aufwand (ROI) ein Sicherheitssystem zu überwinden so hoch ist, dass es sich für einen Kriminellen nicht mehr rechnet einen Versuch zu starten. Die Industrie ist steht's bemüht die Chancen einen solchen Angriffs zu minimieren.

**Man sollte aber ganz klar festhalten dass die meisten erfolgreichen Angriffe im Labor stattfanden – nicht im wirklichen Leben.**

Im Sektor IT Security, erfreut sich die Biometrie eines sehr starken Wachstums, dank der grösseren Verfügbarkeit von preiswerten biometrischen Lesegeräten(Fingerprint Sensoren) die sogar bereits in PC's, PDA's und Mobiltelefone eingebaut sind. Es sind auch schon einige Peripheriegeräte wie Tastaturen und Mäuse mit eingebauten Fingerprintsensoren erhältlich. Die grösste Verbreitung finden allerdings USB Geräte wg. ihrer Flexibilität.

Gesichtserkennung wird auch immer populärer da die meisten Computer heute schon mit der notwendigen Hardware (z.B. digitale Webcam) ausgeliefert werden. Man benötigt dann lediglich eine Softwarelizenz.

Vom Gesichtspunkt der Technologie gesehen besteht ein bestimmtes Interesse in der Grösse des Template und der damit erforderlichen Festplattenkapazität. Im Falle der logischen IT Sicherheit variieren die Templategrößen je nach biometrischer Technologie und welcher Algorithmus genutzt wird.

Wir, von IdentAlink, bieten mit eigenem Algorithmus für serverseitige und clientseitige Verifikation verschiedene biometrische Technologien an; von Gesicht und Iris über Fingerpint können die Technologien multimodal verwendet werden.

Clientseitige Verifikation wird nur in Einzelplatzsystemen verwandt. Serverseitige Verifikation dient der Sicherheit in Netzwerken, Intranets und über das Internet und bietet eine sehr hohe Sicherheit da eine intelligente biometrische engine benutzt wird welche von Zeit zu Zeit die entsprechenden Template anpasst.

Die Anzahl der verwendeten Template(Anwender) oder Netzwerke ist nicht limitiert bzw. richten sich nach der Kapazität der verwendeten Hardware.

**IdentAlink's BioPassport™ Enterprise** Server ist vollkommen Plattformunabhängig und kann nahtlos in bestehende Netzwerke integriert werden.

Überdies, um potentiellen Missbrauch von persönlichen und biometrischen Daten auszuschließen, sind alle Informationen mit einer PKI gesichert. D.h. persönliche Daten und biometrische Daten können nur mit Ihrer Zustimmung (Verifikation) zusammengeführt werden. Zusätzliche kann eine Digitale Signatur ohne Zutun eines fremden „Trust Centers“ genutzt werden.

Dies ist eine sehr begeisternde Zeit für die gesamte Biometrieindustrie. Viele Jahre der Forschung und Entwicklung zahlen sich nun aus und sehr gute und zuverlässige biometrische Lösungen wie IdentAlink's BioPassport™ Enterprise Server werden jetzt am Markt weltweit angeboten. Jetzt da Unternehmen mit großem Namen und Behörden biometrische Lösungen einsetzen, können wir alle sehr zuversichtlich sein das unsere Technologie die Reife und Akzeptanz erlangt die sie

verdient.

*Elmar Hilgers ist der Geschäftsführer und Co-founder von **IdentAlink**. Gegründet in 1997, entwickelte das Unternehmen zuerst Sicherheitslösungen für die englische Gesundheitsindustrie in den Bereichen Arbeitssicherheit und Drogenkontrolle. Die ursprünglich genutzten Technologien der Gesichtserkennung und Fingerprinterkennung wurden mittlerweile durch weitere biometrische Technologien (IRIS, Sprache) erweitert. **IdentAlink** verfügt nun über eine weltweit anerkannte, einzigartige Sicherheitssoftware um zuverlässige Verifikation und Authentikation in verschiedenen globalen Applikationen anzubieten. **IdentAlink's** Verpflichtung zu Forschung und Entwicklung versichert das alle angebotenen biometrische Applikationen stets auf dem neuesten Stand sind und weiter verbessert und ausgebaut werden. Wenn Sie mehr über **IdentAlink** oder den **BioPassport™ Enterprise Server** wissen möchten, laden wir Sie gerne zu einer persönlichen Vorführung in unseren Präsentationsräumen ein.*

*Sie können auch Herrn Elmar Hilgers direkt unter [ehilgers@biometrics.ws](mailto:ehilgers@biometrics.ws) kontaktieren. Zur Vereinbarung einer Präsentation, kontaktieren Sie bitte Frau K. Haase unter [khaase@biometrics.ws](mailto:khaase@biometrics.ws) **IdentAlink GmbH**, Rudower Chaussee 29, 12489, Berlin, Germany. Tel: +49 (0)30 63926973. Fax +49 (0)30 63926971.*