Grundlagen biometrischer Authentifikation

* Marc Ruef

In einer Zeit, in der eine Flut von Passwörter und PINs unser Gedächtnis überfordert und durch sie selbst neue Sicherheitslecks entstehen, sind anwenderfreundliche und sichere Authentisierungsverfahren gefragt. Genau hier kommt die Benutzerverifizierung auf biometrischer Ebene ins Spiel.

Lexikalisch wird die Biometrie als "Lehre der Anwendung mathematischer, statistischer Methoden auf die Mess- und Zahlenverhältnisse der Lebewesen und ihrer Einzelteile" definiert. Im engeren, auf die Informatik-Welt bezogenen Sinn ist Biometrie ein Synonym für den Identitätsnachweis von Personen unter Verwendung ihrer individuellen körperlichen Merkmale. Diese Eigenheiten müssen allerdings so einzigartig ausfallen, dass sie möglichst nur einer Person eindeutig zugeordnet werden können. Fingerabdrükke, Netzhaut- oder Irismuster, Gesichtsform, Stimme oder Venenbild erlauben eine sehr genaue Verifizierung der Echtheit und der daraus resultierenden Kompetenz einer Person. Damit wird der Einsatz dieser Techniken vor allem für Kontrollsysteme sinnvoll, mit deren Hilfe buchstäblich haargenau zwischen berechtigten und unberechtigten Benutzern unterschieden werden muss.

Geschichtliches

Diese futuristisch anmassende Zugangskontrolle siedelt sich in einem noch sehr jungen Gebiet der Informationstechnologie an. Trotzdem können ihre Wurzeln bis ins alte Ägypten zurück datiert werden, als die Pharaonen bestimmte Dekrete mit ihrem individuellen Daumenabdruck signierten.

Die erste bemerkenswerte biometrische Entwicklung wurde im Jahr 1893 von Sir Francis Galton demonstriert, welcher durch seine wissenschaftliche Arbeit belegen konnte, dass keine zwei Fingerabdrücke identisch sind; nicht einmal die von eineiigen Zwillingen. Kurze Zeit später entwarf Sir Edward Henry das nach ihm benannte System, welches auch noch heute in der Kriminalistik in leicht weiterentwikkeltem Zustand Verwendung findet. Henrys System unterteilt die Rillen der Fingerkuppen in acht Kategorien. Durch deren Analyse und den Einbezug von maximal 16 Vergleichspunkten, können Personen eindeutig identifiziert werden. Die früher mittels Tinte durchgeführte Katalogisierung der Fingerabdrücke erscheint primitiv im Vergleich zur heute fortschrittlichen digitalisierten Methode namens "Fingerprint Image Compression Standard", welche die über 200 Millionen Fingerabdrücke in der Datenbank des FBI erst in der aktuell vorliegenden Form möglich machte. Die digitale Fingerabdruckserkennung ist jedoch inzwischen so preiswert geworden, dass manche Firmen sie bereits in ihre Produkte implementieren. Unabhängig voneinander haben Siemens und American Biometric eine Computer-Maus mit Fingerabdruckserkennung auf den Markt gebracht. Etwas unbekannter aber erwähnenswert ist da das Produkt "SecureStart/ISA" von der amerikanischen Firma I/O-Software (www.iosoftware.com), welches den Benutzer vor dem Booten des Systems authentifiziert. Es beinhaltet einen kompakten Fingerabdruck-Scanner, der an eine ISA-Karte angeschlossen wird und mit diversen Betriebssystemen zurecht kommt.

Einzigartige biologische Merkmale

Fingerabdruckserkennung war jedoch erst der Anfang einer zukunftsweisenden Entwicklung. In den letzten Jahren erforschten Wisschenschaftler weitere einzigartige biologische Merkmale des Menschen, welche zur deren Identifizierung verwendet werden können. Von diesen hat das Netzhautmuster am meisten Interesse hervorgerufen. Die Netzhaut (lat. Retina) ist ein äusserst dünnes Gewebe, welches Licht in elektrische Signale umwandelt und über Nervenbahnen zur Abarbeitung an das Gehirn weiterleitet. Die Retina besteht aus insgesamt fünf Schichten, von

Iris-Scan

Bei einem Scan der Netzhaut wird das Auge mit Infrarotlicht bombardiert, wobei die photorezeptiven Strukturen in der Aussenschicht reagieren, indem sie das Licht in ihrem ganz individuellen statischen Muster reflektieren. Solche Abtastungen sind aussergewöhnlich zuverlässig und den Fingerabdrücken in vielen Bereichen überlegen. So wird mit zwischen 700 und 4200 Vergleichspunkte aufgewartet, was dieser Methode eine Einstufung mit extrem hohem Genauigkeitsgrad beschert hat. Das sich schon seit längerem im Einsatz befindliche "IrisScan" ist ein netzwerkfähiges biometrisches Erkennungssystem, welches 256 Workstations pro LAN-Segment unterstützt. Dabei wird die Weiterentwicklung in Form eines Iris-Scans genutzt, der als noch korrekter als ein Netzhaut-Scan gilt. Obwohl "IrisScan" einen NT-Server voraussetzt, kann es zur Absicherung heterogener Netzwerke verwendet werden; Unix-Benutzer werden mit glänzenden Augen danken.

denen zwei durch den Netzhaut-Scanner zur Authentifizierung angesprochen werden (Abbildung 2).

Auch Netzhaut-Scanner und ihre Derivate können in einzelnen Fällen versagen. So funktionieren sie nicht mehr korrekt, wenn der Anwender ganz oder teilweise blind ist oder eine Linsentrübung aufweist. Ausserdem haben diese Systeme eine auffällig hohe Rate an fehlerhaften Zurückweisungen bei berechtigten Personen. Die Gefahr, dass unberechtigte Benutzer authentisiert werden ist zwar gering, doch entsteht oft ein erhöhter Aufwand für alle Anwender mit eigentlich ausreichendem Kompetenzbereich.

Noch neuere Entwicklungen im biometrischen Bereich konzentrieren sich auf die Eigenarten der menschlichen Stimme. Das deutsche Unternehmen DCS (www.dcs.de) brilliert beispielsweise in Zusammenarbeit mit der Firma Biodata Information Technology (www.biodata.ch) mit einem hohen Sicherheitsstandard durch die kombinierte Stimmen-, Lippen- und Gesichtserkennung. Anhand der zusätzlichen Eigenheiten des Gesichtes werden die Bewegungen des Sprechens genauestens überprüft und bei fehlender Berechtigung der Zutritt verwehrt.

Passswort-Falle

Der Vorteil von biometriebasierenden Kontrollen ist schon im geringeren Aufwand für den Endbenutzer zu sehen. Wer hat sich nicht schon mal an ein vergessenes Passwort zu erinnern versucht und in Gedanken ein halbes Duzend seiner PINs sortiert? Noch schlimmer wird es bei notierten Passcodes,

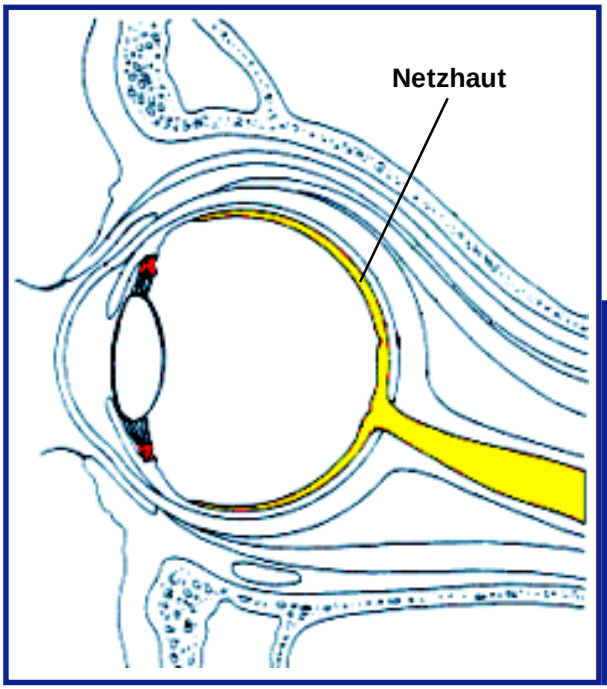


Abb. 1: Die Aussenschicht der Netzhaut enthält reflektierende, photorezeptive Strukturen welche als Zapfen und Stäbchen bekannt sind. Unter diesen, in der Chorioidea-Schicht (Aderhaut) enthält die Netzhaut komplexe Blutgefässsysteme.

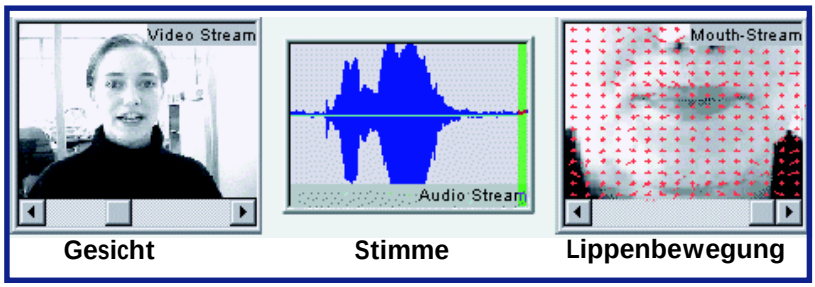
welche von potentiellen Bösewichten missbraucht werden können. Auch Chipkarten-Systeme bergen das Risiko eines Verlusts der Karte auf sich. Der Aufwand zum Ändern oder Sperren betroffener Systeme ist oft zeitintensiv und nervenaufreibend. Diese Zeiten könnten mit der unweigerlich anbrechenden Ära der biometirischen Verfahren vorbei sein, da der Schlüssel zum Schloss wird stets mit sich getragen wird.

Doch wie bei jeder technischen Neuerung reagieren manche Leute mit skepsis. Vor allem die Schützer der Privatsphäre sehen sich auf den Plan gerufen, denn die von Orwell in seinem literarischen Meisterwerk im Jahre 1984 niedergeschriebene

Kombination aus Stimm-, Lippen- und Gesichtserkennung

Die Überprüfung findet wie üblich durch einen Vergleich mit vorangegangenen erfolgreichen Logins statt. Im Falle der Stimme sind dies bestimmte Muster der Zeitintervalle des Sprechens und die Frequenzen der Akustik. Die Sprechbewegungen werden durch das von der Firma DCS patentierte Verfahren der Gesichts-Vektoren überprüft. Ein gewisser Prozentsatz an Übereinstimmungen muss zu der, für den Benutzer erfolgreichen Abarbeitung erreicht werden und lässt sich stufenlos skalieren.

Diese Methode kann ohne Probleme und Einschränkungen in bestehende heterogene Netzwerke implementiert werden und erlaubt eine komfortable zentrale Verwaltung. So werden Logins an Stationen transparent für den Benutzer automatisiert und sicherer. Und das tolle daran ist, dass nur Standard-Videokomponenten, sprich eine handelsübliche Webcam, zur erfolgreichen Nutzung dieser Methode benötigt werden. Eine kostenlose Demo-Version über kann www.bioid.com bezogen werden.



Apokalypse absoluter Kontrolle wird durch die Biometrie ein Stück realer. Eventuelle körperliche Eigenarten, Schäden oder Krankheiten könnten theoretisch ohne das Wissen der Betroffenen erruirt werden und so wiederum dem Missbrauch vorschub leisten.

Schlussfolgerung

Mit einer flächendeckenden Einführung biometrischer Systeme darf in naher Zukunft gerechnet werden. Die grosse Nachfrage nach sicheren Kontrollsystemen und die damit möglich gewordene günstigere Massenproduktion hat dazu beigetragen. Siemens hat mit ihrer leider missglückten ID-Mouse zum ersten Mal ein flächendeckendes Publikum erreicht. Und wenn ich mir die zukunftsträchtige Einschätzung erlauben darf, dann wird es nicht mehr lange dauern bis weitere Unternehmen mit ähnlichen Versuchen ein Teil des neuen Marktes für sich gewinnen wollen. Eine grosse Barriere einer umfangreichen Einführung biometrischer Verfahren wird das Verdrängen der sich mittlerweile etablierten Chipkarten-Standards sein. Trotzdem wird es auch in Zukunft mancher Bereich geben, wo die Plastikkarte als die bessere Variante angesehen werden muss. Ein Zusammenspiel beider Technologien wird besonders in hochsicheren Umgebungen eine nutzbare Kombination sein.

Kontakt:
Marc Ruef
IT-Security Spezialist
E-Mail: m.ruef@biodata.com

Biodata AG
Bahnhofstr. 18
8153 Rümlang
Tel.: 01 880 76 00
Internet: www.biodata.ch