



Richard Sietmann

Augen auf, Finger gezeigt!

Erkennungssysteme auf biometrischer Basis werden praxisreif

Verflixte PIN: lautet sie nun `8015` oder `1580` oder doch eher `0815` ...? Weder noch! Ruckzuck hat der Geldautomat die Karte gefressen. Schon steht man reichlich dumm da, überdies bargeldlos. Identifikationsnummern, Paß- und Kennwörter, überall fordern und überfordern sie unser Gedächtnis. Doch, glaubt man der Industrie, die einen neuen Massenmarkt anvisiert, dürfte es demnächst damit vorbei sein: **einzigartige persönliche Merkmale** (wie Gesicht, Netzhaut, Fingerabdruck) sollen als Sesam-öffne-dich fungieren.

[Unterthema: Handauflegen bei der Einreise](#)

[Unterthema: Risikoverteilung: die Schwachstellen im System](#)

[Unterthema: Der Mensch als Schlüssel?](#)

[Unterthema: Ausgewählte ULRs zum Thema](#)

[Unterthema: PIN-Schutz: Gericht kehrt Beweislast um](#)

Zum Schutz vor Terroranschlägen - Alptraum jedes Veranstalters von Großereignissen - mußten auch bei den Olympischen Winterspielen im japanischen Nagano umfangreiche Sicherheitsvorkehrungen getroffen werden. Dort bewachte beispielsweise ein biometrisches Erkennungssystem den Zugang zur Waffenkammer der Sportschützen: IrisIdent, vom amerikanischen Hersteller IriScan, Inc. (Mont Laurel, New Jersey) installiert, identifizierte die Biathleten individuell am Muster der Regenbogenhaut des Auges.

Computersysteme, die in Sekundenschnelle unveräußerliche Merkmale von Personen zur Identifizierung und Authentifizierung auswerten, haben Konjunktur. Das Sozialamt in Toronto beispielsweise verhindert mit Gesichtserkennungssystemen, daß Bedürftige mehrfach Unterstützung beantragen; deutsche Atomkraftwerk-Betreiber schützen mit Fingerabdrucksensoren Kontrollräume vor ungebetenen Besuchern. Auf dem New Yorker JFK International Airport können Geschäftsreisende lange Schlangen vor der Paßkontrolle umgehen, wenn sie ihre Hand auf ein Lesegerät legen: Stimmt die Handgeometrie mit dem auf einer Chipkarte gespeicherten Muster überein, haben sie die Einreiseprozedur in Sekundenschnelle hinter sich.

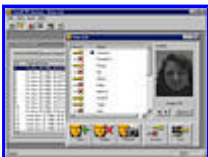


Bild: Visionics Corps.

FaceIt: das Gesicht ersetzt Paßwörter.

Kommt jetzt der Massenmarkt? Ein erstes Einsatzfeld ist der Ersatz von Paßwörtern für den Zugang zu Computern und Netzwerken. Das Gesichtserkennungssystem FaceIt 3.0 der US-Firma Visionics

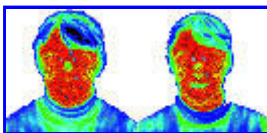
ist inklusive Kamera bereits für 600 Mark kommerziell verfügbar; es sichert den Zugang zum Rechner oder auch zu einzelnen Dateien: Als Wächter für den PC operiert es wie ein Bildschirmschoner und gibt den Weg nach einmaliger Authentifizierung frei; soll eine bestimmte Datei dem Fremdzugriff entzogen werden, läßt man sie auf eine Krypto-Ikone fallen, und bei jedem Aufruf wird dann zunächst die visuelle Erkennung gestartet [1].

Bitte nicht erröten

Als Hardware setzt FaceIt nur eine gewöhnliche Videokamera mit Framegrabber voraus. Vergleichsweise ungewöhnlich geht hingegen die US-Firma TRS Technology Recognition Systems, Inc. (Alexandria, Virginia), an die Gesichtserkennung heran. Sie arbeitet mit Thermogrammen, das heißt, mit dem von einer Infrarotkamera aufgenommenen Profil, das durch die Wärmeabstrahlung der Blutgefäße unter der Gesichtshaut entsteht. Das Produkt wird derzeit unter der Bezeichnung FR1000 auf den Markt gebracht.



Original ...



Bilder: TRS

... und Thermogramm

Wie die visuelle Gesichtserkennung ist das thermogrammetrische Verfahren unaufdringlich, kontaktlos und setzt nicht die Kooperation des Probanden voraus; doch im Unterschied zu den konventionellen optischen Methoden sind die Systeme nicht einmal von der Beleuchtung abhängig und funktionieren sogar im Dunkeln. Dieses Feature dürfte es eher für die polizeiliche Fahndung als für kommerzielle Anwendungen interessant machen. `Eineiige Zwillinge zu unterscheiden macht der Mutter selbst im Hellen Schwierigkeiten, wir schaffen es auch im Dunkeln´, wirbt TRS mit flottem Marketing für das System.

Schwerpunkt Banking

Als zweites Einsatzfeld der Biometrik zeichnet sich die Ablösung des PIN-Schutzes von ec- und Bankkarten ab. Die steigende Zahl von Mißbrauchsfällen und ein vielbeachtetes Urteil des OLG Hamm (s. Kasten `Schlag ins Kontor´) dürften die Entwicklung beschleunigen. Dem Besitzer mehrerer Karten und Konten wird die Vielzahl der PINs schnell lästig; da bringen Schlüssel, die man sich nicht merken muß und die einen dennoch eindeutig ausweisen, eine Erleichterung. Wichtiger noch: Sie autorisieren die Person, und nicht denjenigen, der PIN und Karte in Besitz gebracht hat.

`Die biometrischen Verfahren beobachten wir seit Jahren´, meint Wilhelm Niehoff vom Bundesverband Deutscher Banken in Köln. Seiner Ansicht nach sind sie jedoch `weder einsatzfähig noch in bezug auf Datenschutz und Akzeptanz unproblematisch´. Das sieht die Industrie ganz anders. So stellten Ende letzten Jahres die Chipfabrikanten SGS Thomson, Siemens Halbleiter und Harris Semiconductors die ersten Prototypen von Fingerabdruck-Sensorchips vor. Neben die Tastatur plaziert oder integriert auf einer Chipkarte machen sie die PIN entbehrlich.

Mega-Trend

Die Entwicklung ist unübersehbar: `Die Biometrie gehört zu den zehn Spitzentechnologien, die man in diesem Jahr aufmerksam verfolgen sollte´, empfehlen die Marktforscher der Gartner Group; Wachstumsraten von über 20 Prozent für Biometrie-Produkte haben die Analytiker von Frost&Sullivan beobachtet. Einen weiteren Schub verspricht die Standardisierung, denn bisher sind die Erfassungsgeräte und Vergleichsalgorithmen nicht austauschbar, sondern bilden eine untrennbare Einheit. Die Hersteller liefern nur Komplettlösungen, die nicht interoperabel sind. Folglich halten sich interessierte Anwender mit Investitionen zurück, solange nicht erkennbar ist, welche Technologie sich am Markt durchsetzt, weil sie sich nicht auf ein proprietäres System festlegen lassen wollen.

Diese Sorge wird ihnen jetzt genommen. Anfang Februar legten mehrere Firmen, darunter die britische Forschungstochter IBM Hursley Services & Technology, The National Registry Inc. (Tampa, Florida) und I/O Software (Riverside, Kalifornien), Spezifikationen für Programmierschnittstellen (Application Programming Interfaces, APIs) vor, welche die Integration der biometrischen Sensormodule in unterschiedliche Anwendungsumgebungen erleichtern sollen.

Biometrie-Schnittstellen machen die Hardware austauschbar. Damit kann dann eine Zugangssoftware über eine Oberfläche auf verschiedene Authentisierungsverfahren zugreifen und umgekehrt dasselbe Biometrie-Verfahren von unterschiedlicher Anwendungssoftware genutzt werden. Das schafft Freiräume für Systementwickler und bringt Bewegung in den Markt. `Jetzt, wo IBM und NRI mit den APIs ernst machen, kommt der Stein ins Rollen´, meint der Marktforscher Jackie Fenn von der Gartner Group.

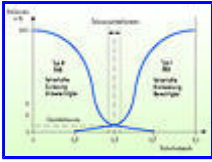


Bild: NRI

NRI legt die Architektur eines biometrischen Authentifikationssystems (BAF/NT) für Windows NT vor (HA = Human Authentication).

Gefördert werden die Bemühungen um offene Standards und mehr Transparenz durch das vom amerikanischen Verteidigungsministerium finanzierte Biometric Consortium, das 1997 ein nationales Testzentrum an der San Jose State University einrichtete. Denn bisher gibt es nur ein einziges herstellerunabhängiges Prüfverfahren, den FERET-Test des US-Army Research Lab (Face REcognition Technology) auf dem Gebiet der Gesichtserkennung. Bei den anderen biometrischen Verfahren ist die Beurteilung der Güte etwa so übersichtlich wie die politische Lage auf dem Balkan.

Insbesondere die Auswertungs- und Vergleichsalgorithmen sind ein sorgfältig gehütetes Geheimnis der Hersteller, die ihr Know-how für sich behalten wollen. `Wenn man die Prospekte der Hersteller biometrischer Produkte liest, weiß man nie, wie die zu ihren Zuverlässigkeitsangaben und Prozentzahlen kommen´, meint ein Insider; `auf Nachfrage herrscht meist betretenes Schweigen.´ Da sind APIs ein erster, wesentlicher Schritt zur Validierung, weil sich mit ihrer Hilfe Sensorhardware und Auswertungsalgorithmen verschiedener Hersteller auf identischen Plattformen gegeneinander testen lassen.



Die Toleranz eines Musterabgleichs biometrischer Systeme wird auf die Gleichfehlerrate eingestellt, wobei beide Fehler minimal sind.

Die Lackmus-Probe des FERET-Tests konnte jüngst eine deutsche Entwicklung, der `PersonSpotter` von der Ruhr-Universität-Bochum, bravourös absolvieren. Bei den Kriterien

- Lokalisieren des Gesichtes im Aufnahmeveld,
- Robustheit gegenüber unterschiedlicher Ausleuchtung,
- Robustheit gegenüber Abweichungen von der Frontalansicht und
- Robustheit gegenüber abnehmender Bildauflösung

setzte er sich gegen starke Konkurrenzprodukte durch - darunter eines vom Massachusetts Institute of Technology (MIT).

PersonSpotter

Der PersonSpotter entstand unter der Leitung von Christoph von der Malsburg und Hartmut Neven und ist eine Weiterentwicklung des als `Bochumer elektronischen Pförtners` bekannt gewordenen Vorläufers ZN-Face [2]. Schon die Qualitäten dieses Programms überzeugten nach der ersten Präsentation 1994 einige Anwender - wie die Deutsche Bank - so sehr, daß sie es als Zutrittskontrolle für ihre Sicherheitsareale einsetzen.

Wie der Vorläufer arbeitet PersonSpotter auf der Basis eines neuronalen Netzes, welches die Merkmale eines Gesichtes und deren räumliche Beziehungen unter anderem mit Hilfe eines `Elastic Graph Matching` aufbereitet. Das Programm besteht aus zwei Modulen. Während die eine Komponente Gesichter in Videosequenzen findet, vergleicht die andere die aufgenommenen mit den in einer Datenbank gespeicherten Konterfeis. Zur Zeit verarbeitet das System zwölf Videobilder pro Sekunde und kann unabhängig von Mimik oder Kopfhaltung maximal acht Personen pro Minute identifizieren.

Auch ein anderes deutsches System, FaceVACS (VACS = Visual Access Control System), wird derzeit in der Praxis getestet. Das von der Dresdener Siemens-Nixdorf-Tochter Advanced Technologies GmbH entwickelte und von plettac electronics (Fürth) vertriebene System abstrahiert aus den von einer CCD-Kamera aufgenommenen Gesichter charakteristische physiometrische Merkmale. Anschließend vergleicht es diese mit den gespeicherten Daten registrierter Benutzer. Ein neuronales Netz bewertet dazu verschiedene Gesichtsgeometrien, insbesondere die Position der Augen zueinander und in Relation zu bestimmten Punkten innerhalb des Gesichts. FaceVACS läuft auf einem Standard-PC unter Windows NT, an Zusatzhardware erforderlich ist eine simple CCD-Kamera mit Framegrabber.

Quantensprung

Biometrische Verfahren, die unverwechselbare und unveräußerliche Merkmale heranziehen, heben die Prüfung von Berechtigungen auf eine neue Stufe.

Der Darmstädter Sachverständige und Gerichtsgutachter Manfred Pausch sieht darin `einen Quantensprung der Sicherheit´ und `die einzige Möglichkeit, wie man die Zugangssysteme wirklich verbessern kann´.

So dienen im elektronischen Zahlungsverkehr PIN und Karte bisher nur der *Autorisierung* - Geld kann beispielsweise jeder abheben, der im Besitz der Karte ist und die Geheimzahl kennt; bis zum Beweis des Gegenteils geht die Vermutung dahin, daß er zur Abhebung befugt ist.

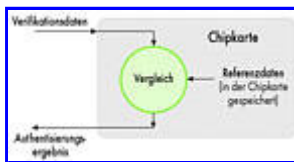


Bild: Struif GMD

Lokale Authentifizierung: Zuerst findet ein Vergleich der biometrischen Meßdaten mit den auf der Chipkarte liegenden Referenzdaten statt, dann wird das Authentisierungsergebnis an das System weitergegeben.

Kommt ein unveräußerliches persönliches Kennzeichen hinzu, wird aus der Autorisierung die *Authentifizierung*, das heißt, es wird anhand des Merkmals geprüft, ob der Nutzer tatsächlich derjenige ist, für den er sich ausgibt. Offensichtlich muß dieses Merkmal eindeutig einer Person zuzuordnen sein - eine Voraussetzung, die biometrische Verfahren sicherstellen müssen. Seine Daten werden mit *einem*, nämlich dem unter seinem Namen abgespeicherten Referenzmuster abgeglichen. Stimmen sie überein, ist der Nutzer authentifiziert.

Bei der *Identifizierung* geht es darum, ein aktuell aufgenommenes Muster mit *allen* in einer Datenbank gespeicherten Referenzmustern zu vergleichen, um daraus die Identität des Betreffenden zu ermitteln. In der polizeilichen Fahndungsarbeit ist das der Normalfall, doch in kommerziellen Anwendungen ist dieser Aufwand entbehrlich. Hier reicht der einfache Abgleich mit dem bei der Anmeldung ausgewählten Referenzdatensatz aus.

Aus dem Blickwinkel des Datenschutzes hat der feine Unterschied gravierende Folgen: Bei der Authentisierung müssen die Referenzdaten nämlich nicht in einer zentralen Datenbank, etwa der Firma oder des Geldinstituts, gespeichert werden, sondern können im Besitz des Mitarbeiters oder Kunden verbleiben und beispielsweise auf der Chipkarte vorliegen.

Nicht weniger wichtig ist die Frage, wo die eigentliche Prüfung erfolgt - lokal auf der Karte oder `im System´. Bei der International Organization for Standardization (ISO) (<http://www.iso.ch>) werden derzeit Architektur und Kommandos für einen lokalen Vergleich von Referenz- und Verifikationsdaten auf Chipkarten spezifiziert. Aber `Stand der Technik ist das noch nicht´, erklärt SmartCard-Experte Bruno Struif von der GMD in Darmstadt, der an den Standardisierungsarbeiten beteiligt ist. Langfristig werden sich wohl nur solche Lösungen durchsetzen, die die Authentisierungsdaten und -prozeduren kontrollierbar in der Rechtssphäre des einzelnen Nutzers belassen, so daß ein Mißbrauch und Datenschutzkonflikte von vornherein ausgeschlossen werden.

Konkurrenz der Technik

Immer mehr Verfahren drängen auf den Markt; die Fülle der Produkte ist inzwischen kaum noch überschaubar. Als individuelle Merkmale lassen sich Gesichtszüge, Sprachproben, Abbilder der Netzhaut oder der Iris, die Handgeometrie, der Fingerabdruck oder die Schreibmotorik bei einer Unterschriftsleistung auswerten. Nicht alle Techniken sind jedoch für Massenanwendungen geeignet; daß ein Bankkunde sich etwa darauf einläßt, am Geldautomaten Sprachproben abzugeben

oder sein Auge an das Okular eines Retina-Scanners hält, damit ein Infrarotstrahl die Netzhaut abtasten kann, ist wohl kaum zu erwarten.

Gesichtserkennungssysteme haben - so sehen es zumindest einige Anwender - den Vorteil, daß sie im Hintergrund ohne aktives Zutun des Betreffenden operieren können. Das bevorzugte Anwendungsgebiet sind Zugangskontrollen zur Unterscheidung von Mitarbeitern und Besuchern, zumal hierbei leicht ein Backup des elektronischen Pfortners möglich ist: Sollte das Erkennungssystem ausfallen, kann ein Mensch problemlos die Identifizierung (wieder) übernehmen, was hingegen anhand der Stimme oder des Fingerabdrucks nur von ausgebildeten Experten zu bewerkstelligen wäre. Ein weiterer Vorteil: Als Hardware ist in der Regel nur eine Standardvideokamera erforderlich. Gewöhnliche PCs sind für Videokonferenzen vielfach schon mit den preiswerten, teilweise in den Monitor integrierten Kameras ausgestattet.

Doch der `harte´ Teil des Erkennungsprozesses liegt in den Auswertungsalgorithmen und der Verarbeitungssoftware. Hier ist die Forschung längst noch nicht abgeschlossen. Während die eine Schule, etwa um Tomaso Poggio am MIT, den Ansatz der Eigenkopfanalyse verfolgt und statistische Abweichungen zu einem oder mehreren künstlich konstruierten `Durchschnittsgesichtern´ bei der Erkennung analysiert, setzt die andere auf die Local Feature Analysis (LFA): FaceIt von Visionics oder der PersonSpotter der Ruhr-Universität ziehen aus einem Satz von Beispielmustern lokaler Merkmale wie Augenabstand oder Mundwinkel und ihrer Lage zueinander nur die markant hervorstechenden zum Vergleich heran und verwerfen die irrelevante Information.

Alle Verfahren müssen zunächst aus der Aufnahme des Gesichtes die wesentlichen Merkmale in einem Referenzmuster extrahieren, um die Komplexität zu reduzieren. Der Merkmalsraum sollte einerseits von niedriger Dimension und der erstellte Datensatz andererseits mit wenigen KByte möglichst klein sein, ohne die Zuverlässigkeit zu beeinträchtigen.

Schlüsselgröße EER

Der Idealfall wäre unabhängig von der unvermeidlichen Variabilität des Gesichtsausdruckes (Mimik, Brille, Frisur, Make-up) und den Aufnahmebedingungen (Beleuchtung, Kopfhaltung) eine 1-zu-1-Beziehung zwischen den erhobenen Verifikationsdaten (der `Identität´) und dem Referenzmuster. Tatsächlich liegt hierin jedoch eine Schwachstelle aller biometrischen Verfahren, denn sie arbeiten alle nach demselben Prinzip.

Die Merkmale speichert man als Referenzdaten ab; sie werden aufgerufen, sobald eine Berechtigung zu prüfen ist. Da bei der praktischen Messung niemals dieselben Bedingungen herrschen, stimmen das aktuell erfaßte Probenmuster und das abgelegte Referenzmuster nie vollständig überein - Gesichtszüge oder Schreibmotorik variieren ebenso wie aufgenommene Fingerprint-Daten. Die zulässigen Toleranzen müssen daher im Auswertungsalgorithmus festgelegt werden.

Das Problem: Bei zu strenger Prüfung werden auch berechtigte Benutzer nicht akzeptiert, was sich kritisch auf die Akzeptanz des Systems auswirkt; lockert man die Schwelle, nimmt man Schäden in Kauf, wenn hin und wieder ein unberechtigter Nutzer abgewiesen wird. Als Maß für die Leistungsfähigkeit eines Erkennungssystems nimmt man die Gleichfehlerrate, bei der die Zahl fälschlich abgewiesener und fälschlich akzeptierter Personen gleichgroß ist. Je niedriger diese Rate liegt, desto besser dürfte das Authentifikationsverfahren sein. Bei den Fingerabdruckprüfungen, wie sie bisher in elektronischen Zugangskontrollen eingesetzt wurden, liegt sie im Promillebereich; für IrisIdent gibt der Hersteller eine um drei Größenordnungen niedrigere Equal Error Rate (EER) von $1 : 1,2 \times 10^6$ an.

BioID

Die Zuverlässigkeit läßt sich steigern, wenn zur Erkennung mehrere individuelle Merkmale

herangezogen werden. Ein solches hybrides System, das Mimik, Stimme und Gesicht zur Einlaßkontrolle heranzieht, hat das Fraunhofer-Institut für integrierte Schaltungen (IIS) in Erlangen entwickelt.

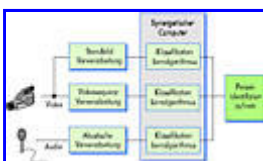
Der nach dem Märchen aus `Tausendundeine Nacht´ benannte Pförtner `SESAM´ - das Akronym steht für `Synergetische Erkennung mittels Standbild, Akustik und Motorik´ - verlangt vom Eintretenden, daß er sich mit seinem Namen vorstellt. Ein gesprochenes Wort reicht für die Erfassung des `Voice Print´ aus. Der charakteristische Stimmabdruck wird dann in seine spektralen Anteile zerlegt und daraus algorithmisch ein Extrakt gebildet, der die analoge Aufnahme mit etwa 4 Kbit digitalisiert.



Bilder: Fhg IIS

SESAM/BioID, der elektronische Pförtner, läßt nur ein, wessen Gesicht, Lippenbewegung und Stimme er erkennt.

Zugleich löst das akustische Signal die eine Sekunde dauernde Videoaufnahme einer Standard-CCD-Graustufen-Kamera aus. Das Volumen der mit einer Auflösung von 768×572 Pixel aufgenommenen Bildinformation - ein Standbild des Gesichts und die Sequenz der Lippenbewegung - muß ebenfalls reduziert werden. Nachdem man die von Fall zu Fall variierende Position von Kopf und Mundpartie kalibriert hat, so daß beide Signale unabhängig von zeitlichen und örtlichen Verschiebungen bei der Aufnahme werden, berechnet das System dazu einen sogenannten optischen Fluß, der die Bewegung einzelner Bildteile durch Vektoren darstellt.



BioID zieht die drei personenspezifischen biometrischen Merkmale Gesicht (statisch), Lippenbewegung (dynamisch) und Stimme (dynamisch) zur Identifikation heran und läßt sich für die verschiedensten Zugangskontrollen einsetzen.

Zur Analyse der Lippenbewegung wird eine Folge von Teilbildern der Mundpartie zu je 128×128 Pixeln aus der Videosequenz extrahiert. Der Algorithmus ermittelt den optischen Fluß aus jeweils zwei aufeinanderfolgenden Bildern der Sequenz und speichert ihn in 16 Feldern zu je 32×32 Vektoren.

Das Standbild wiederum wird durch Translationen und Rotationen so bearbeitet, daß alle aufgenommenen Gesichtspartien dieselbe Größe haben sowie Mund und Augen sich stets in derselben Position befinden, so daß jeder Vergleich von Prüf- und Referenzmuster unter gleichen Bedingungen stattfindet.

Die Kombination von drei unabhängigen Sensorquellen macht die Erkennungsprozedur robust gegen Störungen. Über Änderungen des Erscheinungsbildes, Schnupfen oder Heiserkeit sieht oder hört das System notfalls hinweg: Falls ein Signal aufgrund von Störeinflüssen `verrauscht` ist, erlauben die beiden anderen noch eine sichere Prüfung; wenigstens zwei der drei Merkmalschlüssel müssen den Nutzer übereinstimmend authentisieren.

Das System wird unter dem Namen BioID von dem auf ISDN-LAN-Kopplungen und Sicherheitslösungen spezialisierten Netzwerkhersteller DCS AG in Berlin vermarktet. In der Kombination mit Videokameras soll BioID den Zugang zu Computernetzen absichern, und als Server in bereits vorhandene Videosysteme zur Raum- und Gebäudesicherung eingebunden, dient es als elektronischer Pförtner.

Ihren Augapfel, bitte!

Nur Romantiker sehen die Augen noch als das Fenster zur Seele an - für Sicherheitsingenieure sind auch sie ein unverwechselbares Kennzeichen zur zweifelsfreien Identifizierung. Hierfür bietet die Iris mit ihrer feinzielierten Landschaft aus Punkten, Gruben, Sprenkeln, Streifen, Furchen, verstreuten Fäden und verschlungenen Gefäßen insgesamt 266 biologische Attribute an, die von einer Person zur anderen variieren und die selbst bei eineiigen Zwillingen nicht übereinstimmen.

Der Mathematiker John Daugman von der Universität Cambridge hat die Gleichungen zur Erkennung und Kodierung dieser Charakteristika für das IrisIdent-System entwickelt, das im olympischen Nagano zum Einsatz kam. Aus einem Abstand von etwa 20 cm lokalisiert eine Videokamera bei der Aufnahme die Regenbogenhaut und extrahiert aus ihrem Abbild die Merkmale zu einem 256-Byte-Code. Dazu wird die Iris in acht konzentrische Ringzonen aufgeteilt; das macht die Erkennung unabhängig von der Öffnung der die Lichtmenge regulierenden Blende.

Da eine lebende Pupille ständig in Bewegung ist, läßt sich das System mit einem Glasauge nicht überlisten. Auch nicht mit Kontaktlinsen-Attrappen, die konvex geformt sein müssen, um auf der Hornhaut aufzuliegen, während die Iris an ihrer ebenen Gestalt zu erkennen ist. Auch Brillen oder ungünstige Lichtverhältnisse beeinträchtigen die Erkennung nicht.

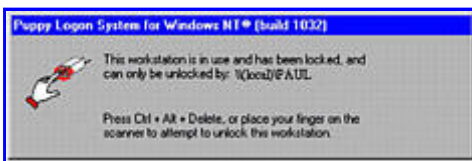
Das patentierte Verfahren der IriScan, Inc., wird von dem amerikanischen Unternehmen Sensor (Moorestown, New Jersey) vermarktet. Als erster Großkunde führt NCR, der Marktführer bei Geldausgabeautomaten, das Authentisierungsverfahren ein. Im Januar begann die englische Nationwide Bank damit, ihre Geldautomaten mit dem IrisIdent-System auszurüsten, um den Kunden die Eingabe der Geheimzahl zu ersparen. Statt dessen genügt der Blick auf den Bildschirm des Automaten, und binnen zwei Sekunden ist die eingescannte Iris mit dem Referenzmuster aus einer Datenbank verglichen.

Fingerabdruck-Verfahren

Eine Alternative am Geldautomaten mit noch größerem Potential für den Massenmarkt stellen Fingerabdruck-Prüfungen dar, die sich allmählich vom negativen Image der erkennungsdienstlichen Behandlung der Polizei befreien. Im Herbst 1997 stellte Sony auf der Comdex die von I/O Software entwickelte Fingerprint Identification Unit (FIU) vor, die die charakterischen Rillen und Riefen der Fingerkuppe optisch erfaßt. Die FIU wird bereits als Paßwortersatz in dem Logon-System der BiometriX International (Wien) für Windows-NT-Rechner eingesetzt, das komplett etwa 1400 Mark kostet.

Aus den aufgenommenen `Bildern` destilliert ein Erfassungsprogramm in rund 1000 Bytes die sogenannten Minuzien heraus - Linienenden, Verzweigungen, Schlingen und Wirbel, die auch in der Daktyloskopie (Fingerabdruck-Verfahren) zur zweifelsfreien Identifizierung dienen: Die Wahrscheinlichkeit, daß zwei Menschen identische Fingerabdrücke haben, wird auf unter eins zu

einer Milliarde geschätzt; selbst Zwillinge lassen sich damit unterscheiden.



Bilder: BiometriX

Die von Sony vorgestellte Fingerprint Identification Unit arbeitet mit dem Logon-System von BiometriX International zusammen und ersetzt bei Windows NT Login und Paßwort.

Anders als Sony setzen die Chiphersteller SGS Thomson, Harris Semiconductors und Siemens Halbleiter auf eine mikroelektronische Lösung. Ihre Fingerabdruck-Sensoren erfassen das Linienmuster der Fingerkuppe im unmittelbaren mechanischen Kontakt, ohne daß ein optischer oder mechanischer Adapter - wie etwa ein Scanner oder eine Kamera - zwischengeschaltet werden muß: Wird der Finger auf die Siliziumfläche des Chips gelegt, nehmen Sensorzellen die Änderungen des elektrischen Feldes auf, das die erhabenen Linien und die Vertiefungen auf der Fingeroberfläche hervorrufen, und erzeugen daraus sein elektrisches Abbild.

Der 'Fingertip-Sensor', den Siemens kürzlich auf der OmniCard in Berlin vorstellte, besteht aus einem Feld von insgesamt 256×256 Sensorelementen und hat eine Flächenauflösung von $50 \mu\text{m}$ beziehungsweise 500 dpi. Er kann etwa 50 Graustufen unterscheiden und erfüllt alle heute üblichen Standards für Fingerabdruck-Erkennungssysteme. Mit Abmessungen von $12,8 \times 12,8 \text{ mm}^2$ hat dieser Sensor etwa die Größe einer kleinen Briefmarke und enthält zugleich einen A/D-Wandler, der die Bilddaten am Sensorausgang in digitaler Form zur Verfügung stellt.



Bild: Siemens

Nicht mehr als eine halbe Sekunde braucht der Siemens Fingertip-Sensor zur Erfassung des Fingerabdrucks.

Die Erfassung beruht auf einem kapazitiven Meßprinzip. Jedes Pixel stellt einen Kondensator dar, und die Haut des aufgelegten Fingers wirkt als dritte 'Kondensatorplatte', wobei sich durch die Erhöhungen und Vertiefungen der Rillenmuster in den einzelnen Sensorelementen unterschiedliche Rückkoppelungskapazitäten ergeben. Die analogen Werte liefern auf diese Weise eine

dreidimensionale Aufnahme des Abdrucks, so daß etwa ein Foto anstelle eines echten Fingers sofort auffiele. Da überdies die Leitfähigkeit der Haut das Signal beeinflusst, ist der Sensor auch mit einer Wachs-Attrappe nicht zu täuschen.

Das in Verbindung mit der auf einem Laptop installierten Erkennungssoftware demonstrierte System beeindruckt durch seine Geschwindigkeit: Die Verifikation des Nutzers benötigt etwa eine halbe Sekunde. Die ersten Produkte sollen noch in diesem Jahr auf den Markt kommen. Dabei ist zunächst, wie Projektleiter Thomas Scheiter erklärt, an die Autorisierung des Zugangs zu Laptops und Mobilfunk-Handys gedacht. Der Leiter des Produktgebiets Chipkarten- und Sicherheits-ICs bei Siemens Halbleiter, Ulrich Hamann, hält es langfristig sogar für denkbar, den Sensor in die Enter-Taste des PC zu integrieren: Jede Eingabe, die mit `Enter` abgeschlossen wird, ließe sich dann mit einer Berechtigungsprüfung verbinden.

Mit dem Siemens-Sensor (aber auch mit den entsprechenden Sensoren anderer Firmen) arbeitet tipChip, ein Fingerabdruck-Erkennungssystem der Voxel Systems GmbH, zusammen, das von den beiden Entwicklern Dr. Joachim Dengler und Bern Lind erstellt wurde. Fertig ist bereits ein Windows- und Unix-Logon. Die Fingerabdrücke werden dazu einmal eingelesen, anschließend unverwechselbare Merkmale errechnet, die sich entweder in einer Datenbank oder auf einer Chipkarte speichern lassen. 120 bis 200 Bytes reichen, so die Entwickler, pro Fingerabdruck aus. Beim Einloggen legt man seinen Finger auf den Sensor, der zu prüfende Abdruck wird dann mit den gespeicherten verglichen und bei Übereinstimmung der Daten der Zugang erlaubt. Die Verifikation kann direkt auf der Chipkarte stattfinden. Sollte das Ganze in Massenproduktion gehen, rechnet die Firma mit einem Endpreis, der um 350 Mark liegen soll.

Die Bergdata AG aus Bonn setzt den FingerChip von Thomson-CFS ein, der sich durch ein Thermoverfahren auszeichnet. Auch hier werden eindeutige Merkmale extrahiert, die sich ebenfalls auf dem Chip speichern lassen.

Eine ganz andere Vorgehensweise hat ein Team der polnischen Firma Optel (aus Wroclaw) gewählt: es arbeitet mit Ultraschall. Berührt beispielsweise die zu identifizierende Fingerkuppe eine Kontaktfläche, wird sie seitlich per Ultraschall bestrahlt. Die kontaktgestreuten Wellen empfängt ein Schallwandler, der eine Ringbewegung ausführt, deren Achse senkrecht zur Kontaktoberfläche steht. Aufgenommen werden können so die oberflächennahen Strukturen der papillaren Linien, die für die Entstehung der Fingerabdrücke verantwortlich sind.

Fernziel: Chip-Integration

Das ultimative Ziel ist die Kombination des Sensors mit Prozessor und Speicherbausteinen auf einer Chipkarte. Damit würde die Authentisierung *vollständig* auf einem abgesetzten Teilsystem durchgeführt. `Das wird noch vier bis fünf Jahre dauern`, warnt SmartCard-Experte Bruno Struif von der GMD jedoch vor überzogenen Erwartungen. Denn einer solchen Integration steht noch die Baugröße des Sensors entgegen.

Bisher ist der Siemens-Prototyp nur zu Demonstrationszwecken in eine knapp 4 mm dicke Plastikkarte eingebettet worden - ein Vielfaches der mit 0,76 mm genormten SmartCards. Zudem beschränken die SmartCard-Standards der ISO 7810 wegen der mechanischen Zerbrechlichkeit der Siliziumträger die Grundfläche einzelner Karten-ICs auf 25 mm², und kleiner als auf eine halbe Briefmarkengröße läßt sich der Sensor nicht miniaturisieren, weil mindestens diese Fläche für die Aufnahme der Minuzien benötigt wird. Vorerst findet man daher den Fingerprint-Sensor nur an Tastaturen oder Kartenterminals.

Schreibmotorik

Vielleicht kommt der elektronische Geschäftsverkehr ja auch ohne Chipkarten aus, wenn sich der am

belgisches Mikroelektronikzentrum IMEC in Leuven entwickelte SMARTpen durchsetzt - ein biometrisches Mikrosystem, das eine handschriftliche Unterschrift in eine elektronische Signatur transformiert. Der 'intelligente' Kugelschreiber wertet mit seinen hochkomplexen Innereien aus Sensoren, AD/DA-Wandlern und ASICs zur Signalverarbeitung, Batterie und einem winzigen Sender, der als drahtlose Schnittstelle zum Rechner fungiert, die nutzertypische Motorik beim Unterschreiben aus. Die Fälschungssicherheit beruht deshalb nicht auf dem grafischen Erscheinungsbild des Schriftzuges, sondern dem dynamischen Schreibverhalten des Nutzers.

Die Sensoren nehmen die Kräfte und Beschleunigungen in drei Dimensionen sowie die Neigung auf, und die Auswertelogik extrahiert daraus anhand der Form, der Schreibdynamik und des Neigewinkels die individuellen Merkmale der Unterschrift. Vergleichbare Systeme gab es bislang nur in Verbindung mit einem Digitalisieretableau; der SmartPen kann jedoch mit gewöhnlichem Papier genutzt werden; die einzige Voraussetzung ist eine feste Unterlage. Die Meßdaten werden verschlüsselt an den Computer übertragen.



Bilder: LCI

SMARTpen: Elegantes Äußeres, kompliziertes Innenleben

In Produktionsstückzahlen soll sich der Preis nach Angaben der LCI-Computer Group in Hertogenbosch (Niederlande), die den IMEC-Kugelschreiber vermarkten wird, zwischen 50 und 250 Dollar bewegen. Der SMARTpen ist aufgrund der aufwendigen Innereien zwar noch etwas klobiger als das gewohnte Schreibgerät, aber feingestylte Designer-Kulis sind ohnehin nicht jedermanns Sache.

Mit jedem normalen Schreibstift arbeitet HESY, das Handschriften-Erkennungssystem für Normalstifte von René Baltus und Marc-Bernd Woop. Allerdings bedarf es einer besonderen Unterlage: einem auf vier Drucksensoren gelagerten Tablett. Bevor es ernst, das heißt, die Unterschrift geprüft wird, muß zunächst ein Kennfeld, das aus den vier Dimensionen Länge, Breite, Druck und Zeit besteht, erstellt werden. Dies errechnet ein entsprechendes Lernprogramm aus mehreren Probeunterschriften. Als erkannt bewertet das System später nur die Unterschriften, deren Werte innerhalb dieses Kennfelds liegen. Bei jeder erkannten Unterschrift geht zugleich ein gewisser Anteil der Daten in das Kennfeld ein, somit regiert das System flexibel auf eine sich im Lauf der Zeit verändernde Unterschrift. HESY kostet momentan etwa 2500 Mark, bei einer Massenproduktion erhoffen sich die Bonner Hersteller, den Preis auf 500 bis 200 Mark pro Stück drücken zu können.

An Alternativen zur zweifelsfreien Authentisierung mangelt es jedenfalls nicht. Welche biometrische Technik in der Akzeptanz der Nutzer das Rennen macht, bleibt daher spannend - wie auch die Frage, ob sie dann nicht nur den Zwillingstest besteht, sondern künftig auch geklonte Doppelgänger unterscheiden kann. (ae)

Literatur

[1] Karl Sarnow: Gesicht statt Paßwort, FaceIt: visuelle Identifikation am PC daheim, c't 12/97, S. 60

[2] Patrick Hamilton, Die maschinelle Gesichtserkennung wird praxisreif, c't 2/97, S. 86

Kasten 1

Handauflegen bei der Einreise

Auch deutsche Geschäftsreisende, die mehr als dreimal jährlich in die USA fliegen, können durch Handauflegen die Einreiseformalitäten beschleunigen. Nähere Informationen und Anträge zur Teilnahme am Immigration and Naturalization Service Passenger Accelerated Service System (INSPASS) sind unter

Inspass
P.O. Box 300 766
JFK Airport Station
Jamaica, NY 11430
(0 01) 7 18/2 44-37 22

erhältlich. Erste Tests der Handscanner in Verbindung mit einer Chipkarte begannen 1993 auf dem New Yorker Kennedy-Airport, dem Newark International Airport und dem Pearson International Airport im kanadischen Toronto. Gegenwärtig machen etwa 65 000 Vielflieger davon Gebrauch. In diesem Jahr soll INSPASS auf acht weiteren Flughäfen Nordamerikas eingesetzt werden: Chicago, Honolulu, Houston, Los Angeles, Miami, Montreal, San Francisco und Vancouver.

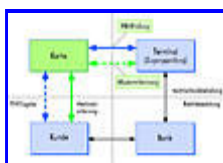
Kasten 2

Risikoverteilung: die Schwachstellen im System

Jeder Zugriffs- oder Zugangsschutz stützt sich auf eine Kombination von Besitz (Karte, Schlüssel), Wissen (PIN oder Paßwort) oder (biometrisches) Merkmal.

Der PIN-Schutz zur Sicherung von Kartenanwendungen beruht auf Wissen, das übertragbar ist. Andererseits ist dafür die technische Abwicklung der PIN-Prüfung einfach und eindeutig.

Weil biometrische Merkmale nicht übertragbar sind, ist die Zuordnung von Karte und Inhaber im Prinzip eindeutig. Hier ist allerdings der Ausgang der Zugangsprüfung mit Unsicherheiten der Erkennungsalgorithmen behaftet. Da bei der Aufnahme der Merkmale nie dieselben Bedingungen herrschen, stimmen das aktuell erfaßte Probenmuster und das abgelegte Referenzmuster in der Regel nicht überein. Mathematische Algorithmen und Erkennungssoftware können beim Vergleich der Verifikationsdaten mit den Referenzdaten daher nur innerhalb bestimmter Toleranzen die Übereinstimmung feststellen.



Die kritischen Schnittstellen der Authentifizierung: Die PIN (blau) ist leicht zu prüfen, aber übertragbar, deshalb bleibt die Zuordnung der Karte zum Inhaber eine Schwachstelle (blau gestrichelt) des Gesamtsystems. Biometrische Merkmale erlauben zwar die eindeutige Personifizierung, sie verlagern aber die Schwachstelle in die Verifikationsalgorithmen bei der

Zugangsprüfung.

Diese Toleranz wird je nach Anwendung festgelegt. `Bei einer Kreditkarte muß man aus Gründen der Akzeptanz auf jeden Fall vermeiden, daß der berechtigte Benutzer nicht an sein Geld kommt - mit der Gefahr, daß hin und wieder auch ein unberechtigter Nutzer durchrutscht´, beschreibt ein Fachmann eines namhaften Chipkartenherstellers das Problem. Bei der Zugangsprüfung in den Kontrollbereich eines Kernkraftwerks sieht das anders aus, `da akzeptiert der berechtigte Nutzer eher, auch einmal versehentlich abgewiesen zu werden´.

Mit biometrischen Verfahren verlagert sich das Restrisiko in jedem Fall auf den Systembetreiber. Wer seinen PC auf diese Weise schützen will, ist das in der Regel selbst. Spätestens, wenn einen der eigene Rechner hartnäckig abweist und den Zugang zum Arbeitszeug verwehrt, dürfte man ins Grübeln kommen.

Kasten 3

Der Mensch als Schlüssel?

Neue und vermeintlich untrügliche Sicherheitssysteme führen stets auch zu neuen Formen der Kriminalität. Ausgefeilte technische Systeme sind immer nur die eine Seite der Medaille, und der Gewinn an Sicherheit hier ist möglicherweise trügerisch. Die Fälle häufen sich, in denen Opfer unter Körpereinsatz am Geldautomaten zur Abhebung gezwungen oder ihnen die Geheimzahl abgepreßt wurde. Müssen wir künftig anstelle irgendeines Paßworts in wahrsten Sinne des Wortes unseren Augapfel hüten oder um die Fingerkuppe bangen? Und obwohl es derzeit eher nach Science-fiction klingt, hätte auch die Gentechnologie einiges beizusteuern, den paßgerechten Klon zum Beispiel. Die Erfahrung zeigt jedenfalls: Wo ein krimineller Wille ist, bahnt er sich seinen Weg. Wer den Menschen selbst zum Schlüssel macht, sollte daher nicht vergessen, daß mit Gewißheit versucht wird, auch diesen in Besitz zu bringen. Auf welche Weise auch immer.

Kasten 4

Ausgewählte ULRs zum Thema

Organisationen	Biometric Consortium	http://www.biometrics.org
	National Biometric Test Center	http://www-engr.sjsu.edu/~graduate/biometrics
	Smart Card Resource Center	http://www.smart-card.com/page10.html
	TeleTrust Deutschland eV	http://www.teletrust.de
	Bundesamt für Sicherheit in der Informationstechnik (BSI)	http://www.bsi.bund.de
Gesichtserkennung		
visuell	Ruhr-Universität Bochum	www.neuroinformatik.ruhr-uni-bochum.de
	ZN-Bochum GmbH	www.zn.ruhr-uni-bochum.de
	Visionics Corp.	http://www.faceit.com , http://www.softline.de
	plettac electronic security GmbH	http://www.plettac-electronics.de/
	SNI Siemens Nixdorf	http://www.snat.de/nc6/face.htm

	Miros, Inc.	http://www.miros.com
Thermogramme	Technology Recognition Systems, Inc.	http://www.betac.com/trs
	Unisys	http://www.unisys.com/marketplace
Augen		
Retina	EyeDentify, Inc.	(0 01) 5 04/9 27-42 90
Iris	IriScan, Inc.	http://www.iriscan.com
	Sensar, Inc.	http://www.sensar.com
Handgeometrie	Recognition Systems, Inc.	http://www.recogsys.com
	Biomet Partners, Inc.	http://www.webconsult.ch/biomet.htm
	IBM Global Government Industry	http://www.government.ibm.com/gov/ais.nsf
Fingerabdruck		
Chips	SGS-Thomson	http://www.st.com
	Siemens Halbleiter	http://www.w2.siemens.de/semiconductor
	Harris Semiconductor	http://www.semi.harris.com
Systeme	I/O Software	http://www.iosoftware.com/fiu/
	Optel	E-Mail: optel@optel.com.pl
	BiometriX International	http://www.user.xpoint.at/biometrix
	Who Vision Systems	http://whovision.com
	Biometric Identification	http://www.BiometricID.com
	RJM Rheinmetall Elektronik	http://www.rjm-jena.de/fingerprint.htm
	Identicator Technology Corp.	http://www.identicator.com
	The National Registry, Inc.	http://www.nrid.com
	Identix, Inc.	http://www.identix.com
	SAC Technologies, Inc.	http://www.sacman.com
	Voxel Systems GmbH	E-Mail: j.dengler@dkfz-heidelberg.de
	Bergdata AG	http://www.bergdata.com
Sprache	Keyware Technologies, Inc.	http://www.keywareusa.com
	Sensory, Inc.	http://www.sensoryinc.com
	Speakerkey	http://www.speakerkey.com
	ABS GmbH	Fax: 0 36 41/67 54 10
	Voice Control Systems	http://www.voicecontrol.com/products.html
Motorik		
Unterschrift	IMEC	http://www.imec.be
	LCI Computer Group NV	http://www.lcigroup.com
	R. Baltus	Fax: 02 28/25 81 36
Tastenanschlag	Net Nanny Software International, Inc.	http://www.netnanny.com
Hybrid-Verfahren	DCS Dialog Communication Systems AG	http://www.dcs.de

Kasten 5

PIN-Schutz: Gericht kehrt Beweislast um

Der vierstellige Zahlencode der Persönlichen Identifikationsnummer (PIN), der mehr als 40 Millionen ec-Karten und rund 20 Millionen Bankkarten autorisiert, hat einen gravierenden Nachteil: Er läßt nicht erkennen, wer ihn tatsächlich benutzt. Der PIN-Schutz beruht auf Wissen, und das ist übertragbar - ein Risiko, das sich in der Regel der Nutzer zurechnen lassen muß.

Wenn ein Dieb unter Verwendung der PIN Geld abheben konnte, galt dies bislang meist als Anscheinsbeweis, daß der Karteninhaber die Geheimzahl nicht sorgfältig genug verwahrt hatte; er mußte nun den Nachweis führen, daß der Täter nicht durch seine grobe Fahrlässigkeit an die Geheimzahl gelangt war, wenn er von der Bank den Schaden ersetzt haben wollte. Solange der Täter nicht gefaßt und der Weg der Information rekonstruiert werden konnte, blieb das praktisch unmöglich.

Unter der Annahme, daß das PIN-Verfahren sicher ist, wird so das Restrisiko auf die Nutzer abgewälzt. Schlimmer noch: Wer den Verlust der Karte und den Schaden anzeigt, läuft Gefahr, selbst wegen Versicherungsbetrug oder Vortäuschen einer Straftat angezeigt zu werden.

Im Frühjahr letzten Jahres kehrte das Oberlandesgericht Hamm in einer wegweisenden Entscheidung (Az: 31 U 72/96; NJW 25/97, S. 1711-1713) die Beweislast erstmals um: Danach ist die Verletzung der Sorgfalts- und Mitwirkungspflichten durch den Kunden `von der Bank darzulegen und zu beweisen ..., da nicht auszuschließen ist, daß der Täter die PIN selbständig durch Ausprobieren oder Entschlüsseln anhand der auf der Karte gespeicherten Daten ermittelt haben kann´.

Die PIN wird aus den Kartendaten - Kontonummer, einem Teil der Bankleitzahl, Kartenfolgenummer - errechnet. Dazu werden diese Daten zunächst mit dem Algorithmus des Data Encryption Standard (DES) unter Verwendung eines geheimen Schlüssels chiffriert und aus dem Verschlüsselungsergebnis dann die PIN abgeleitet.

Die Sicherheitsphilosophie der Banken, die die Rechtsprechung zuvor stets unbesehen übernommen hatte, beruht darauf, daß die Berechnung der PIN im wesentlichen dem Brechen des DES-Algorithmus gleichkäme. Bei dem 56stelligen DES hieße das, unter 2^{56} Möglichkeiten den richtigen Schlüssel herauszufinden. Einmal erfolgreich, könnten Ganoven mit dem Generalschlüssel von jeder gestohlenen ec-Karte binnen kurzem die dazugehörige Geheimzahl ermitteln.

Im letzten Jahr gelangt es erstmals einer internationalen Gruppe, genannt `Bovine RC5 Effort´, in Zusammenarbeit mehrerer zehntausender Computer via Internet, durch `brute force´ einen 56 Bit langen DES-Schlüssel zu knacken. Dabei handelte es sich allerdings nicht um den Master-Key des ec-Kartensystems, sondern um die Lösung einer mit 10 000 Dollar dotierten Preisaufgabe der kalifornischen Firma RSA Data Security, die damit auf die Schwächen der symmetrischen Verschlüsselung nach dem DES-Standard aufmerksam machen wollte (<http://www.rsa.com/>).

Sicherheitsanalysen zeigen jedoch, daß die eigentliche Schwachstelle woanders liegt. So beträgt die rechnerische Wahrscheinlichkeit, aus einem vierstelligen Zahlencode die richtige PIN zu ermitteln, keineswegs 1 : 10 000. Aus der Art, wie die PIN bei den rund 40 Millionen im Umlauf befindlichen ec-Karten aus Bankleitzahl und Kontonummer zugeteilt wurde, könnte ein sachkundiger Angreifer die Erfolgsquote schon auf 1 : 150 erhöhen, bevor er weitere technische Hilfsmittel einsetzt.

Grundsätzlich stellen Ratestrategien, so Werner Schindler, Mathematiker und Kryptographie-Experte beim Bundesamt für Sicherheit in der Informationstechnik (BSI), `einen ernstzunehmenden Angriff gegen das ec-Kartensystem dar´. Doch daraus eine pauschale Rechtsprechung zu Gunsten oder zu

Ungunsten des Bankkunden abzuleiten, sei `nicht gerechtfertigt'. Er plädiert dafür, daß die Gerichte stets einen Sachverständigen zu Rate ziehen, der den konkreten Einzelfall beurteilt.

Das dürfte teuer werden, denn mit der zunehmenden Beliebtheit der Karten als Zahlungsmittel steigt auch der Mißbrauch. 1992 verzeichnete die Statistik des Bundeskriminalamtes 9080 Straftaten mittels rechtswidrig erlangter Karten für Geldausgabe- und Kassenautomaten; 1996 hatte sich die Zahl auf 26 802 bei einer Schadenssumme von 33 Millionen Mark verdreifacht.

Der Zentrale Kreditausschuß (ZKA) der deutschen Banken- und Sparkassenverbände hält das Verschlüsselungssystem der ec-Karten jedoch nach wie vor für sicher. Entgegen anderslautenden Presseberichten habe in keinem konkreten Fall eine Entschlüsselung des Codes nachgewiesen werden können, ließ er Ende letzten Jahres verlauten.

Tatsächlich hätten wohl, um die hohen Investitionskosten wieder einzuspielen, die Mißbrauchsfälle `epidemieartig ansteigen' müssen, meint Schindler, `wofür es heute keine Anzeichen gibt'.

Gleichwohl werden derzeit neue vierstellige PINs für alle im Umlauf befindlichen ec-Karten berechnet, die mit den Mängeln der statistischen Ungleichverteilung aufräumen sollen. Ferner sollen die PINs im Triple-DES-Verfahren verschlüsselt werden, wobei jede Filiale einen eigenen 112-Bit-Institutsschlüssel erhält und nicht mehr wie vordem auf den zentralen 56-Bit-DES-Pool-Schlüssel zugreifen muß. Zudem sollen die Karteninhaber von diesem Jahr an eine vier- bis zwölfstellige Ziffernfolge selbst als PIN festlegen können.

`Das PIN-Verfahren ist in der Öffentlichkeit zu Unrecht als zu schwach dargestellt worden', erklärte Abteilungsleiter Wilhelm Niehoff vom Bundesverband deutscher Banken im Februar auf einer Veranstaltung des BSI in Bonn. Wenn durch die öffentliche Diskussion das Vertrauen in die Sicherheit untergraben werde, bevor ein adäquater Ersatz durch biometrische Systeme für den Masseneinsatz zur Verfügung stehe, würde man nur in eine `Zeitfalle' geraten. Das System könne `auch durch künstlich erzeugtes Mißtrauen ruiniert werden'.