

■ ■ ■ Biometrie – Fluch oder Segen?



Jürgen Kühn
Senior Consultant

Frankfurt, 2.2.2011

trivadis
makes IT easier. ■ ■ ■

Kurzvorstellung



Jürgen Kühn

Senior Consultant

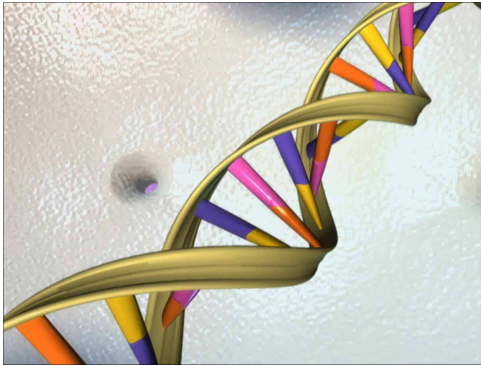
Dipl.-Ing. Nachrichtentechnik UNI Duisburg
Seit 1.8.2005 bei Trivadis
Identity and Access Management
Single Sign-On
Smartcards
Biometrie
PKI

Agenda



- Grundlagen
- Fingerprint
- Irisscan
- Gesichtserkennung
- Gefahren
- Diskussion

Biometrie im Alltag



Was ist Biometrie



- "Wissenschaft von der Zählung und [Körper]messung an Lebewesen"
- Aus dem Griechischen
- Bios = Leben
- Métron = Maß
- Biometrie ist eine Technik zur Authentifikation und Identifikation von Personen anhand von spezifischen Körpermerkmalen



Quelle: DUDEN - Das große Fremdwörterbuch

Merkmale zur biometrischen Identifikation (1)



Eigenschaften von Merkmalen zur biometrischen Identifikation

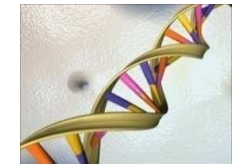
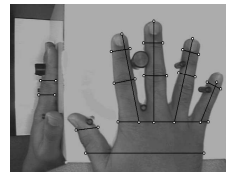
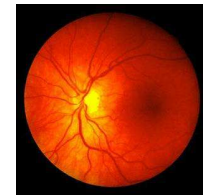
- **Universalität**
 - Merkmal ist bei jeder Person vorhanden
- **Einzigartigkeit**
 - Merkmal ist bei jeder Person anders
- **Permanenz**
 - Merkmal ändert sich über die Zeit nicht oder nur minimal
- **Erfassbarkeit**
 - Merkmal lässt sich quantitativ erheben

Merkmale zur biometrischen Identifikation (2)



■ Physiologisches Merkmal

- Fingerabdruck
- Gesicht
- Iris
- Retina
- Handgeometrie
- Venenmuster
- Ohrgeometrie
- DNA



■ Verhaltensbasiertes Merkmal

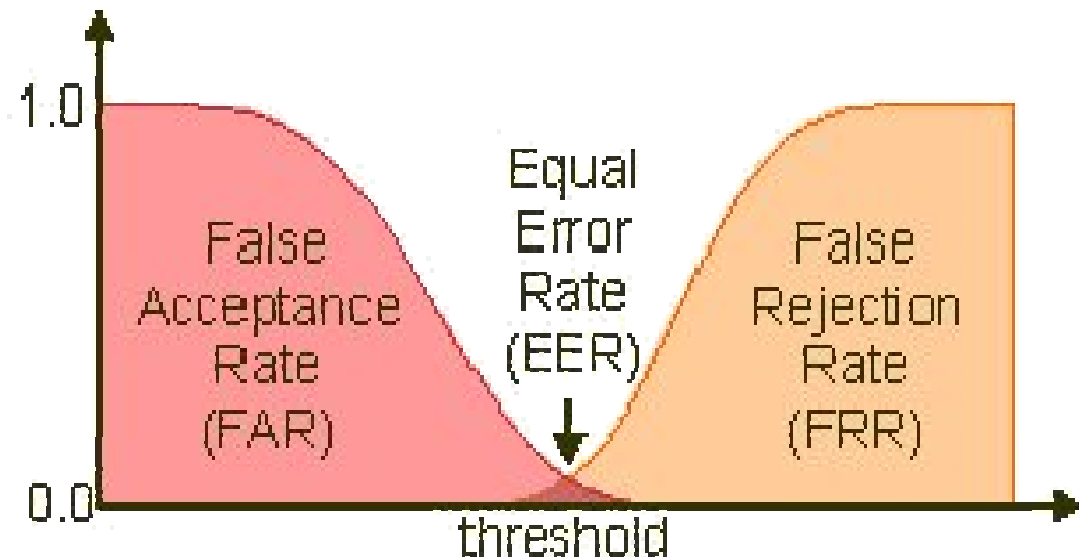
- Unterschrift (dynamisch / statisch)
- Gestik / Mimik beim Sprechen
- Gang
- Stimme / Sprechverhalten
- Tippverhalten an der Tastatur



FAR und FRR (1)



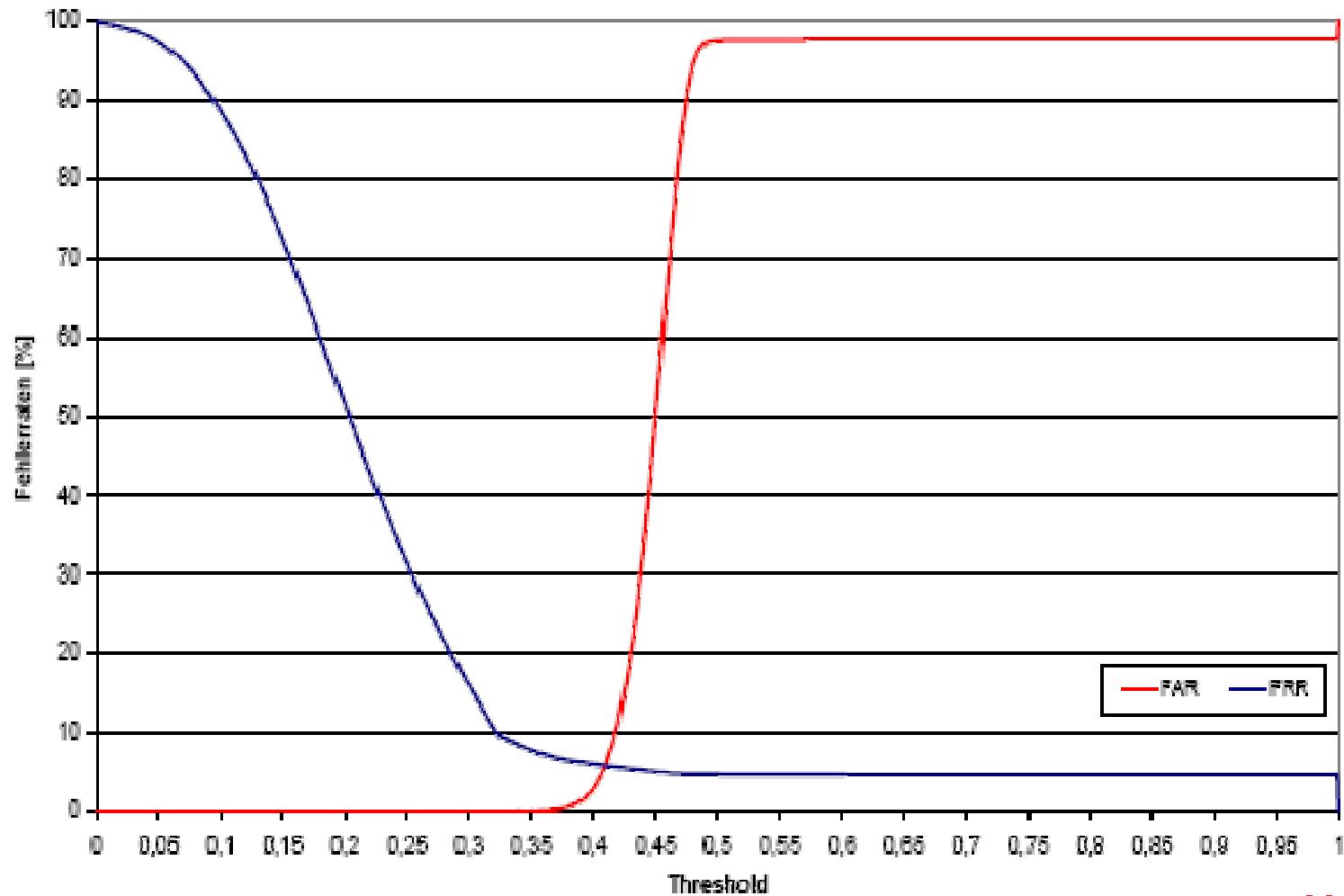
- Nur eine Wahrscheinlichkeit der Übereinstimmung
- False Acceptance Rate FAR
 - Rate der unberechtigt akzeptierten Personen
- False Rejection Rate FRR
 - Rate der unberechtigt zurückgewiesenen Personen
- Equal Error Rate ERR
 - $FAR = FRR$
- threshold bestimmt, ob das System "sicher" oder "komfortabel" ist



FAR und FRR (2)



- Praxis



Verifikation und Identifikation



■ Verifikation

- Prüfen gegen nur eine Referenz

■ Identifikation

- Prüfen gegen beliebig viele Referenzen
- Wahrscheinlichkeit für Falscherkennung steigt exponentiell mit Anzahl der Referenzen

■ Mehrere Versuche bei einer Referenz

- Bei 2 Versuchen und FAR = p

$$p(2) = p + (1-p) p$$

- Bei n Versuchen und FAR = p

$$p(n) = p + (1-p)*p + (1-p)*(1-p)*p + \dots = 1 - (1-p)^n$$

FAR = 0,002
N = 200, P(N) = 32%
N = 2000, P(N) = 98%
N = 10000, P(N) = 99.999%

Agenda



Daten sind
immer im Spiel.

- Einleitung
- Fingerprint
- Irisscan
- Gesichtserkennung
- Gefahren
- Diskussion

Fingerprint: Funktionsweise (1)



■ Sensortypen

- Optisch
- Kapazitiv
- Thermisch
- Ultraschall
- Druck

■ Verfahren

- Pattern matching über das gesamte Bild
- Minutienbasiert
- Verfolgen der Papillarsegmente
- Position der Schweißporen

■ 20-30 Merkmale

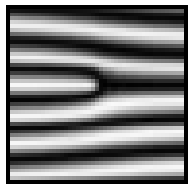
- Selbst bei eineiigen Zwillingen unterschiedlich
 - Bei DNA nicht



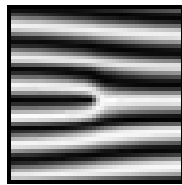
Fingerprint: Funktionsweise (2)



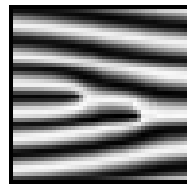
- Minutien



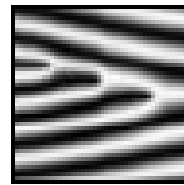
Linienende



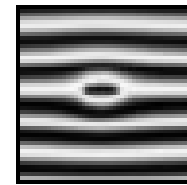
Gabelung



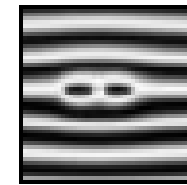
Gabelung
zweifach



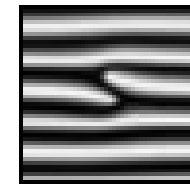
Gabelung
dreifach



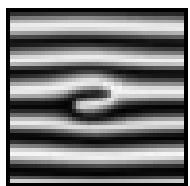
Wirbel



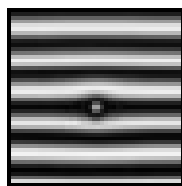
Wirbel
zweifach



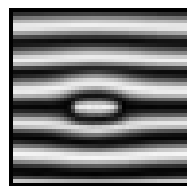
Seitliche
Berührung



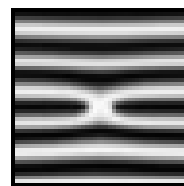
Haken



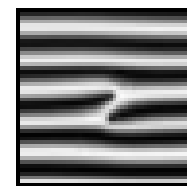
Punkt



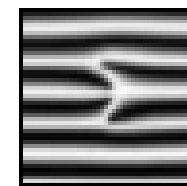
Intervall



X-Linie



Brücke



Brücke
zweifach



Fortlaufende
Linie

Quelle: BSI, „Evaluierung biometrischer Systeme Fingerabdrucktechnologien – BioFinger“, öffentlicher Abschlussbericht

Fingerprint: Lebenderkennung



- Messung des Blutsauerstoffgehalts durch Bestimmung der Hämoglobinkonzentrationsverhältnisse auf Basis der unterschiedlichen Absorption von unterschiedlichen Infrarotlicht-Wellenlängen
- Puls
- Elektrischer Widerstand der Haut
- Temperatur
- Reflexionseigenschaften im Ultraschallbereich
- Blutdurchfluss

Fingerprint: Leser



Standard



Ultraschall



BioAPI



kapazitiv



integriert



optisch

Fingerprint: Schwachstellen (1)



- Latenzbildreaktivierung
 - Anhauchen
 - Graphitpulver
 - Farbpulver

- Anfertigen einer Fingerabdruckkatrappe
 - Gelatine
 - Holzleim

- Verwenden der Latenzabdrücke
 - Graphitpulver und Tesa



Fingerprint: Schwachstellen (2)



- Authentisierung am Computer
- Video "Fälschung des Fingerabdrucks und Nutzung einer Attrappe zur Anmeldung am Notebook" entfernt

Fingerprint: Vor- und Nachteile



- sehr gut erforschtes Verfahren
 - hohe Einzigartigkeit des Merkmals
 - billige Sensoren
 - Verfahren zur Identifikation geeignet
-
- gute Lebenderkennung relativ aufwendig
 - hygienische Bedenken
 - 5% aller Personen haben keine sinnvoll nutzbaren Fingerabdruckmerkmale
 - nicht fälschungssicher



Agenda

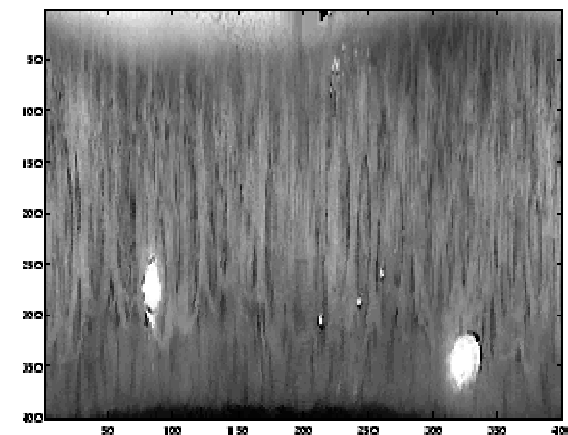
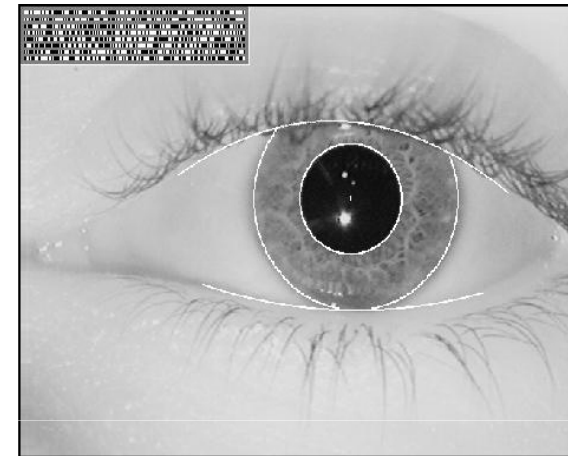


- Einleitung
- Fingerprint
- Irisscan
- Gesichtserkennung
- Gefahren
- Diskussion

Iris Scanner: Funktionsweise



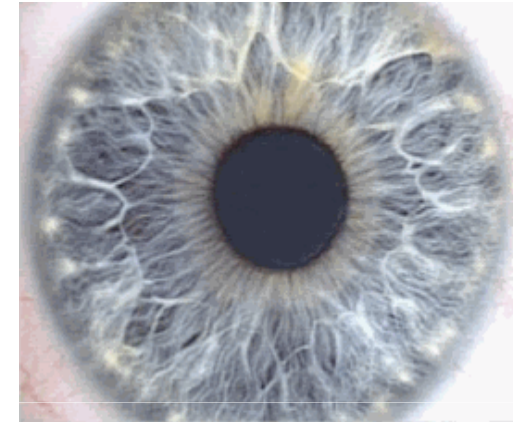
- Anstrahlen mit Infrarotlicht
- Makroaufnahme des Auges im nahen Infrarotbereich (680-850 nm)
- Extraktion der Iris
- Aufteilen der Iris in 8 kreisförmige Abschnitte
- Erkennung markanter Muster (Corona, Krypten, Fasern, Flecke, Narben, radiale Furchen, Streifen)
- Erzeugen des Iriscodes
 - Gabor Wavelet Transformation
 - 244 Merkmale
 - 256 Bytes (mit Maskenbits 512 Byte)



Iris Scanner: Funktionsweise



- Ein weltweit genutzter Algorithmus
 - John Daugman, University of Cambridge
- Iris nach 25 Jahren nicht unterscheidbar
- Selbst bei eineiigen Zwillingen unterschiedlich
- Gute FAR und FRR
- Keine Erkennung von Krankheiten oder Drogenkonsum möglich
- Lebenderkennung
 - Einstrahlung und Reflektion
 - Pupillenreflex
- Schnelle Erkennung
- Aktive und passive Systeme



Iris Scanner: Leser



Computerzugang



Kiosk System



Gebäudezugang

Iris Scanner: Schwachstellen



- Überlistung mit Foto oder Inkjetausdruck
- Vorspielen einer Videosequenz
- Kontaktlinse mit gedruckter oder handgemalter Iris
- Kontaktlinse mit Irishologramm
- Mit Lebenderkennung kaum Überlistung möglich



Iris Scanner: Vor- und Nachteile



- hohe Einzigartigkeit
- hohe zeitliche Konstanz
- einfache Lebenderkennung durch Pupillenreflex
- Verfahren zur Identifikation geeignet

- Merkmalsveränderung durch Krankheit
- Beleuchtung, Brille, Kontaktlinsen
- Kosten
- Nutzerakzeptanz
- Benutzerverhalten bei aktiven Systemen



Agenda



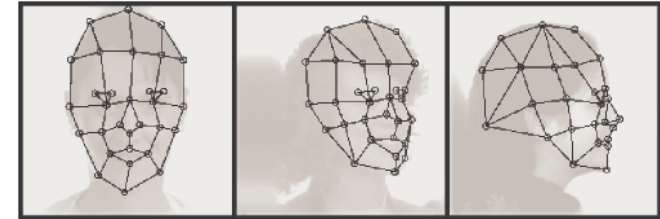
Daten sind
immer im Spiel.

- Einleitung
- Fingerprint
- Irisscan
- Gesichtserkennung
- Gefahren
- Diskussion

Gesichtserkennung: Funktionsweise



- Merkmalsbasierte Gesichtererkennung
 - Extraktion einzelner Merkmale
 - Klassifizierung anhand dieser Merkmale
 - Elastic Bunch Graph Matching
 - Erkennung anhand geometrischer Merkmale
- Holistischer Ansatz
 - Betrachtung des kompletten Gesichts
 - Template Matching
 - Fourier-Transformation
 - Eigenface-Methode
- Kombinationen aus obigen Verfahren



Quelle: Automatische Gesichtserkennung: Methoden und Anwendungen, Dominikus Baur, Universität München

Gesichtserkennung



- Verwendet werden vor allem solche Merkmale des Gesichts, die sich aufgrund der Mimik nicht ständig verändern
 - obere Kanten der Augenhöhlen
 - die Gebiete um die Wangenknochen
 - die Seitenpartien des Mundes.

- Normalisierung mit Hilfe markanter Punkte im Gesicht
 - z.B. Nase, Augen, Mund, Kinn
 - Rotation
 - Translation
 - Skalierung des Kopfes

- 3D Gesichtserkennung
 - Streifenprojektion
 - Erkennungsleistung noch unterhalb der 2D Verfahren
 - (Forschungs-) Ansätze

- Interoperabilität gemäß ISO/IEC 19794-5

- FRR mit 1 % mittlerweile akzeptabel
 - 1993 noch 79%

Gesichtserkennung: Schwachstellen



- Verkleidung
 - Maskenbildner
 - Sonnenbrille
 - Brille
- Fotografie
- Videosequenz
- Kunstkopf

- Schlechte Beleuchtung
- „Grimassen“



Gesichtserkennung: Vor- und Nachteile



- Hohe Benutzerfreundlichkeit
- Hohe Akzeptanz
- Gesicht ist immer (wenigstens teilweise) sichtbar
- Kann unbeobachtet aufgenommen und überprüft werden

- Geringe relative zeitliche Konstanz
- Niedrige Einzigartigkeit
- Keine Kooperation erforderlich
- Kann unbeobachtet aufgenommen und überprüft werden



Vergleich der Verfahren



Merkmal	Fingerprint	Iris Scan	Gesichts- erkennung
Eindeutigkeit	?	10e-78	?
FAR	0,01 - 0,2 %	0,0001 %	0,1 %
FRR	0,1 - 5 %	1 %	1 % (1993: 79%)
Merkmale	25	244	22
Akzeptanz	-	- -	+ +

Agenda



Daten sind
immer im Spiel.

- Einleitung
- Fingerprint
- Irisscan
- Gesichtserkennung
- Gefahren
- Diskussion

Fiktion ?



- Video "Applikation eines Fingerabdrucks zur Beweisfälschung" entfernt

Gefahren (1)



- Verlust des biometrischen Merkmals
 - Nicht-Ersetzbarkeit

- Fingerabdruck
 - Sicherheit
 - Eindeutig
 - nicht fälschungssicher
 - Beweislast
 - Kriminaltechnische Konsequenzen
 - Rechtliche Konsequenzen

- Technikgläubigkeit
 - Fingerabdruck von Wolfgang Schäuble
 - Einkaufen mit Fingerprint
 - Mörder bringen gezielt fremde DNA mit (Studie)

Gefahren (2)



- Einkaufen mit Fingerprint
- „Ökonomie der Kriminalität“
- Video "Einkaufen mit Fingerprint Attrappe" entfernt

$$\begin{aligned} \text{FAR} &= 0,002 \\ N = 200, P(N) &= 32\% \\ N = 2000, P(N) &= 98\% \\ N = 10000, P(N) &= 99.999\% \end{aligned}$$

Quelle: Planetopia 25.1.2009

ePass (1)



- Gespeichert im optisch maschinenlesbaren Bereich:
 - Vornamen, Familienname, ausstellender Staat, Passnummer, Geschlecht, Geburtsdatum und Ablaufdatum des Passes

- Im kontaktlosen Chip des Passes wird das Passfoto gespeichert

- Zwei Fingerabdrücke
 - seit November 2007 zusätzlich im Chip gespeichert
 - flach, nicht gerollt
 - als komprimierte Bilder gespeichert

- Keine Speicherung bei Einwohnermeldeämtern
 - anders als zuvor vom damaligen Bundesinnenminister Wolfgang Schäuble vorgeschlagen



ePass (2)



- Die genaue Nutzung und Speicherung der ausgelesenen Daten an Grenzen ist unklar
- Unverschlüsselte Übertragung der Passdaten per Funk
- Funkchips ermöglichen eine unbemerkte Überwachung und Verfolgung einzelner Personen
- Erhöhung der Fälschungssicherheit könnte auch ohne Speicherung von personenbezogenen Daten realisiert werden
- Studie des BSI wies die Unausgereiftheit der Technik bei biometrischen Verfahren im Alltag nach
 - Eine Abweisungsrate von 3 bis 23 Prozent
 - Gesonderte Untersuchung der zurückgewiesenen Personen
 - Untragbarer personeller Mehraufwand

ePass (3)



- Linksfraktion kritisiert Biometrie-Strategie der Bundesregierung

Die Bundesregierung hat nach Angaben der Linksfraktion im Bundestag eingeräumt, dass "biometrische Verfahren allenfalls sekundär zur Früherkennung von terrorverdächtigen Personen" herangezogen werden können (13.01.2009)

- EU-Parlament segnet Kompromissvorschlag zu biometrischen Reisepässen ab

Eine Grenze für die nationalen Regierungen hat allerdings kürzlich der Europäische Gerichtshof für Menschenrechte mit seiner Entscheidung gegen die britische Regierung (Marper vs. UK) gesetzt. Darin hatte der EUGH die Speicherung von DNA-Daten und Fingerabdrücken für unverhältnismäßig und unvereinbar mit dem Artikel 8 der Europäischen Menschenrechtskonvention erklärt. Etwaige nationale Gesetze zu den biometrischen Datenbanken fänden hier ihre EU-rechtliche Grenze (15.1.2009)

ePass (4)



- Erfolgsgeschichte "EasyPass" soll fortgeschrieben werden
 - 38.500 Flugpassagiere passierten die automatische Grenzabfertigung
 - Nur 17.500 wurden zum biometrischen Personencheck zugelassen
 - 20 Prozent der vom System abgelehnten Passagiere besaßen keinen elektronischen Reisepass, waren nicht volljährig oder kamen aus nicht zugelassenen Ländern
 - 28 Prozent legten den Pass falsch in das Lesegerät ein
 - 7 Prozent der Fälle versagte die Funkkommunikation, mit der das auf dem Pass gespeicherte biometrische Bild in das Grenzprüfsystem übertragen wird
 - Von den 17.500 Nutzern, die vom Lesegerät akzeptiert wurden, konnten 15.000 nach dem Bildabgleich ohne weiteres einreisen
 - Mit einer Erfolgsquote von 87,5 Prozent sei EasyPass als Erfolg zu werten, erklärte Nuppeney
 - In nur 5,6 Prozent aller Fälle versagte die automatische Gesichtskontrolle
 - Die verbleibenden 8,7 Prozent der Passagiere blickten nicht richtig in das Kamerasystem, das nach einer Größenmessung des Nutzers so lange versucht, optimale Gesichtsfotos zu schießen, bis die Verifikation geglückt ist oder ein Timeout erfolgt
 - "False Acceptance Rate" von 0,1 Prozent
 - 10.10.2010

Quelle: www.heise.de

Seltsames (1)



- Cat Stevens
 - Wenn man mal in einer Datei landet...

- Phantom von Heilbronn
 - 40 Tatorte mit identischen DNA Spuren
 - "verschiedene DNA-Treffer der 'Unbekannten weiblichen Person' (UwP) im Zusammenhang mit Sachverhalten, die aus kriminalistischer Sicht nicht mehr plausibel waren"
 - Verunreinigung der zur Probenaufnahme verwendeten Wattestäbchen durch DNA eines Mitarbeiters

- Biometrische Gesichtserkennung für Laptops gehackt
 - Überwindung des Systems mit einem Foto eines registrierten Benutzers
 - Mit gefälschten Gesichtsbildern durch Erzeugung einer hohen Anzahl an Bildern
 - Von den Laptop-Herstellern fordern die Sicherheitsexperten, die biometrische Authentifizierung von den Geräten zu entfernen und alle Nutzer vor dem Gebrauch der Funktion zu warnen



Seltsames (2)



- Wikileaks am 30.11.2010
- US-Außenministerin Hillary Clinton soll ihren Botschaftern im Juli 2009 geheime Direktiven erteilt haben, ... biometrische Daten wichtiger UN-Beamter zu erheben.
- Auf Clintons Wunschzettel standen unter anderem Passwörter und Verschlüsselungs-Keys, die hochrangige UN-Mitarbeiter für die offizielle Kommunikation nutzen, sowie Kreditkarten- und Vielfliegernummern.
- Darüber hinaus sollten US-Diplomaten in der Demokratischen Republik Kongo, Uganda, Ruanda und Burundi sogar Fingerabdrücke, DNA-Proben und Iris-Scans bestimmter Zielpersonen aus UN-Kreisen sammeln.

Seltsames (4)



Wir entdecken unseren Körper

Knochen sind das Gerüst unseres Körpers



... und von dir.



Ferse



ANNA

TIBO

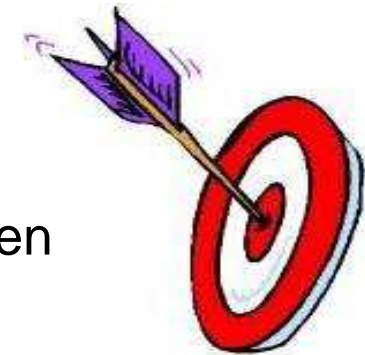
HELEN

Kein Mensch auf der Welt hat genau die gleichen Fingerabdrücke wie du. Wie sieht dein Daumenabdruck aus?

Fazit



- Biometrische Systeme können die Sicherheit erhöhen
- Voraussetzung ist eine mustergültige Umsetzung
- Biometrische Systeme können umgangen werden
- Gespeicherte biometrische Daten wecken Begehrlichkeiten
- Beweiskraft könnte juristisch angezweifelt werden



*„Wir sind nicht nur verantwortlich für das, was wir tun,
sondern auch für das, was wir nicht tun“*

(Voltaire)

■ ■ ■ Vielen Dank!



?

www.trivadis.com

trivadis
makes IT easier. ■ ■ ■



Basel · Baden · Bern · Lausanne · Zürich · Düsseldorf · Frankfurt/M. · Freiburg i. Br. · Hamburg · München · Stuttgart

Weitere Informationen



- <http://www.biotrust.de/>
- <http://www.biometrie-online.de/>
- <http://www.bsi.bund.de/literat/studien/BioFinger/index.htm>
- Behrens/Roth „ Biometrische Identifikation“
- EU-Studie: „Usability of Biometrics in Relation to electronic signatures“
- <https://berlin.ccc.de/index.php/Biometrie>
- <http://www.google.de>
- <http://www.wikipedia.de>