

■ ■ ■ Biometrie



Jürgen Kühn
Security Consultant

Frankfurt, 28.1.2009

trivadis
makes IT easier. ■ ■ ■

Kurzvorstellung



Jürgen Kühn

Security Consultant

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

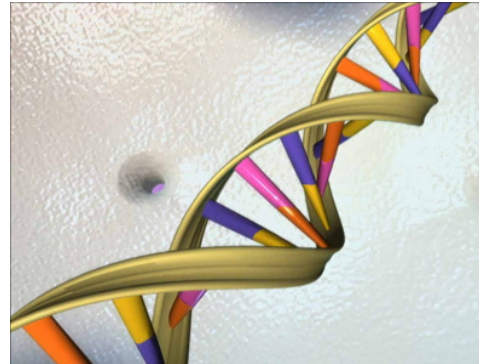
Agenda



Daten sind
immer im Spiel.

- Einleitung
- 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



- **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



- Physiologisches Merkmal
 - Fingerprint
 - Gesicht
 - Iris
 - Retina
 - Handgeometrie
 - Venenmuster
 - Ohr
 - DNA

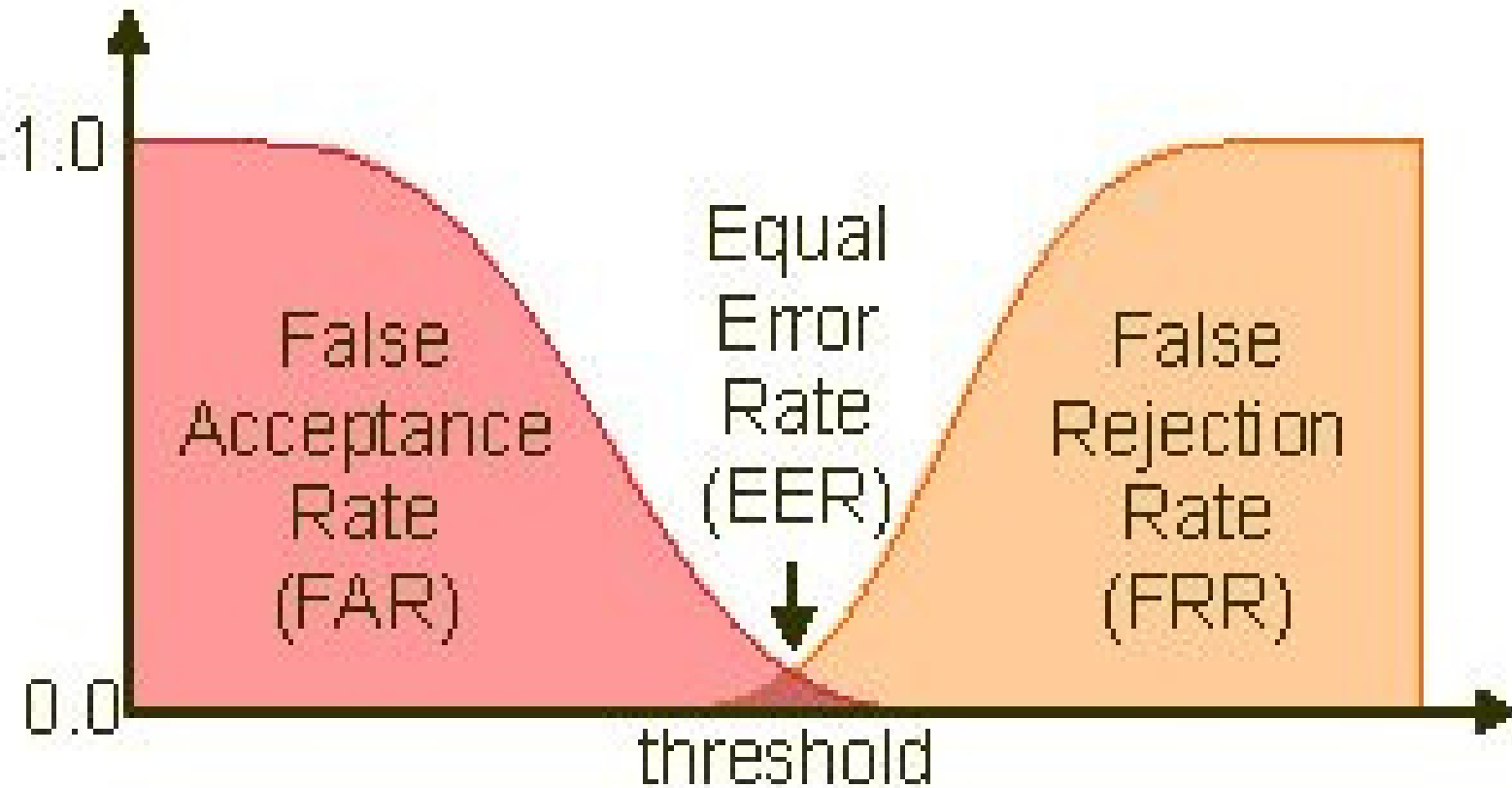
- Verhaltensbasiertes Merkmal
 - Unterschrift (dynamisch/statisch)
 - Gestik / Mimik beim Sprechen
 - Gang
 - Stimme / Sprechverhalten
 - Tippverhalten an der Tastatur

Grundlagen

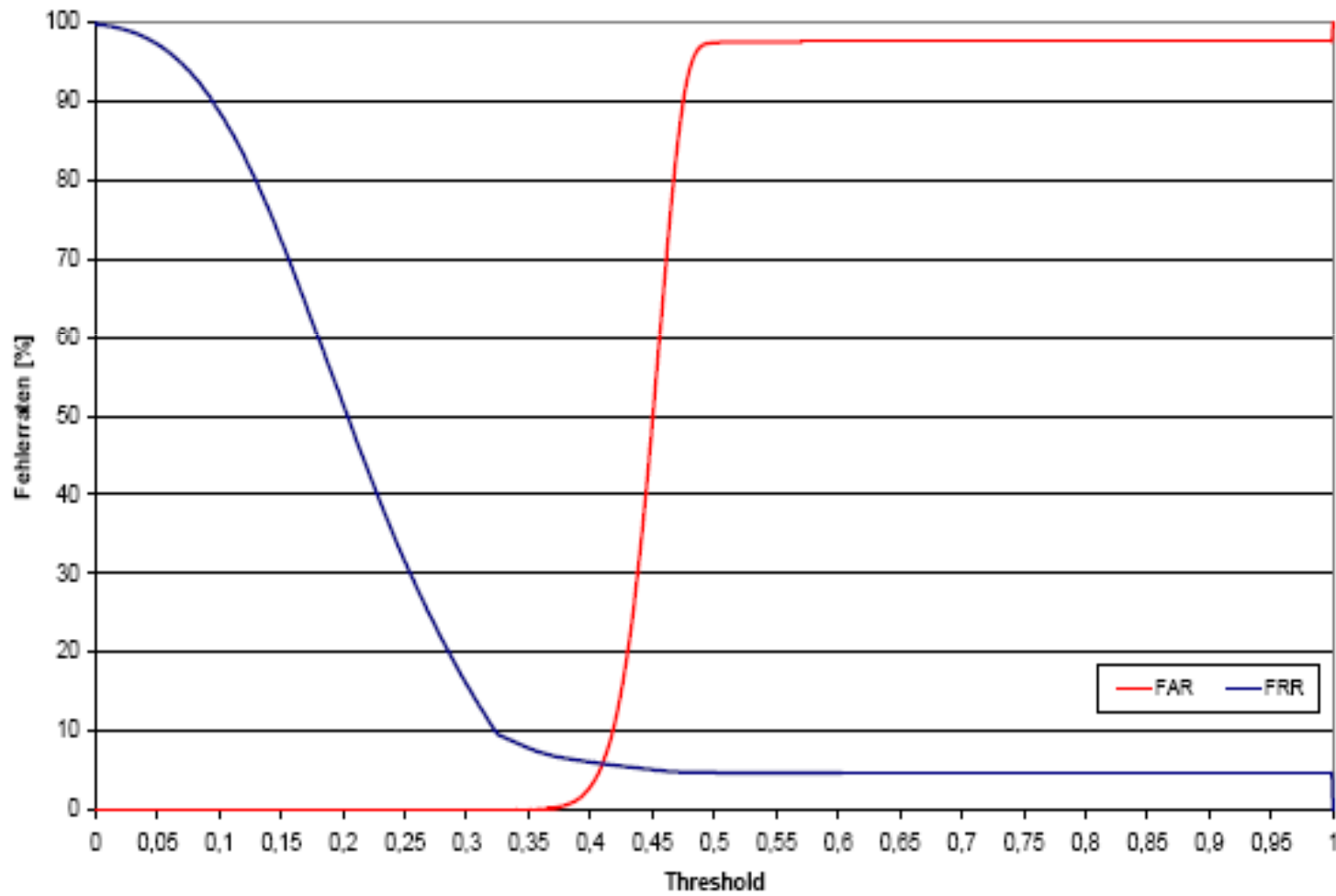


- Nur eine Wahrscheinlichkeit der Übereinstimmung
- False Acceptance Rate FAR
 - Rate der unberechtigt akzeptierten Personen
- False Rejection Rate FRR
 - Rate der unberechtigt zurückgewiesenen Personen
- Equal Error Rate ERR
 - $FAR = FRR$
- Verifikation
 - Prüfen nur gegen eine Referenz
- Identifikation
 - Prüfen gegen beliebig viele Referenzen
 - Wahrscheinlichkeit für Falscherkennung steigt exponentiell mit Anzahl der Referenzen

FAR und FRR (Theorie)



FAR und FRR (Praxis)



Agenda



Daten sind
immer im Spiel.

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

Fingerprint: Funktionsweise



■ Sensortypen

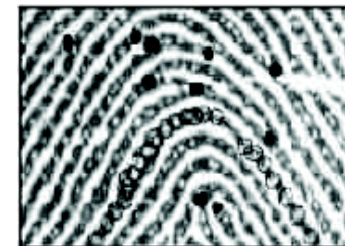
- Optisch
- Kapazitiv
- Thermisch
- Ultraschall
- Druck

■ Verfahren

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

■ 20-30 Merkmale

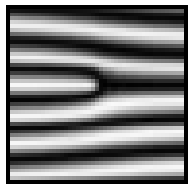
- Selbst bei eineiigen Zwillingen unterschiedlich
 - Bei DNA nicht



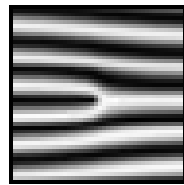
Fingerprint: Funktionsweise



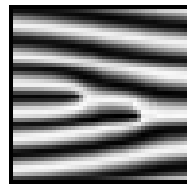
- Minutien



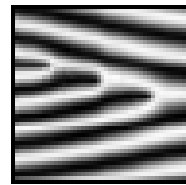
Linienende



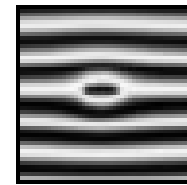
Gabelung



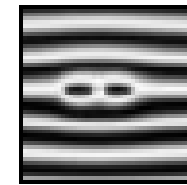
Gabelung
zweifach



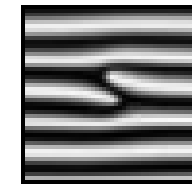
Gabelung
dreifach



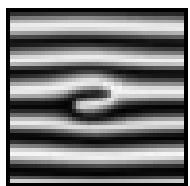
Wirbel



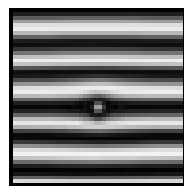
Wirbel
zweifach



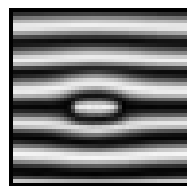
Seitliche
Berührung



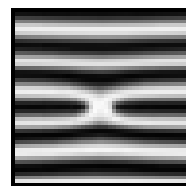
Haken



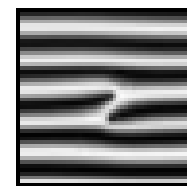
Punkt



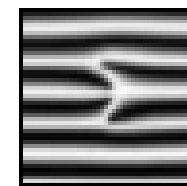
Intervall



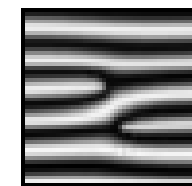
X-Linie



Brücke



Brücke
zweifach



Fortlaufende
Linie

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

Fingerprint: Lebenderkennung



- Puls
- elektrische Eigenschaften der Haut (spezifischer Widerstand)
- Farbe der Haut
- Absorptionseigenschaften im Infrarotbereich
- Reflexionseigenschaften im Ultraschallbereich
- Schweißaustritt

Fingerprint: Marktsituation



Standard



Ultraschall



BioAPI



kapazitiv



integriert



optisch

Fingerprint: Schwachstellen



- Latenzbildreaktivierung
 - Anhauchen, Graphit- oder Farbpulver
- Anfertigen einer Fingerabdruckatrappe
 - Gelatine oder Holzleim
- Verwenden der Latenzabdrücke
 - Graphitpulver und Tesa
- Authentisierung am Computer
- Einkaufen mit Fingerprint



Fingerprint: Schwachstellen



- Video:
- Authentisierung am Computer
- Fälschen eines Fingerabdrucks

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



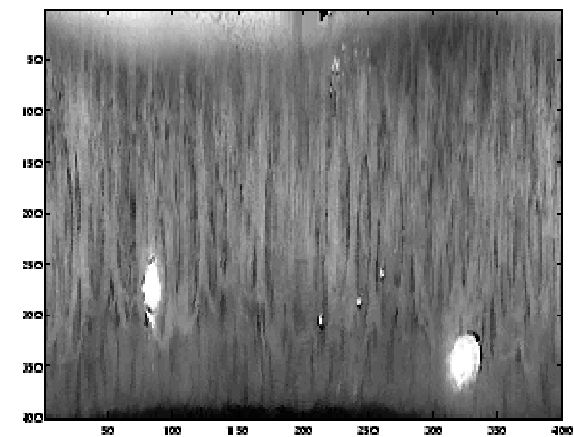
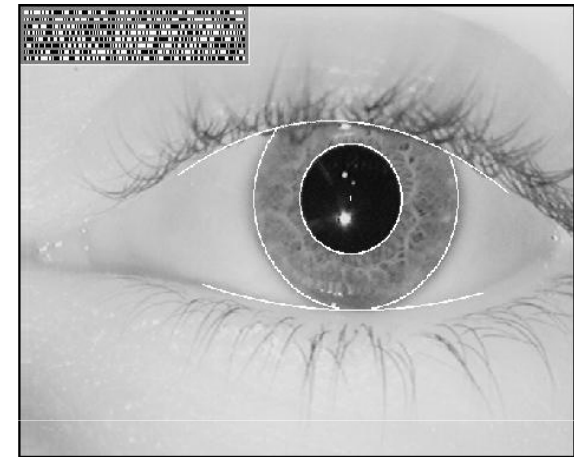
Daten sind
immer im Spiel.

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

Iris Scanner: Funktionsweise



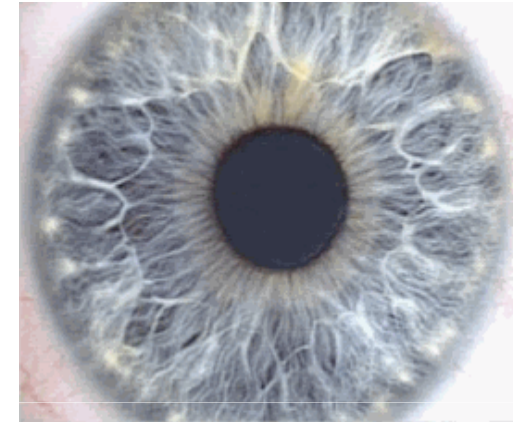
- Anstrahlen mit Infrarotlicht
- Makroaufnahme des Auges im nahen Infrarotbereich (680-850 nm)
- Extraktion der Iris
- Aufteilen der Iris in 8 kreisförmige Abschnitte
- Erkennung markanter Muster (Corona, Krypten, Fasern, Flecke, Narben, radiale Furchen, Streifen)
- Erzeugen des Iriscodes
 - Gabor Wavelet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



Iris Scanner: Funktionsweise



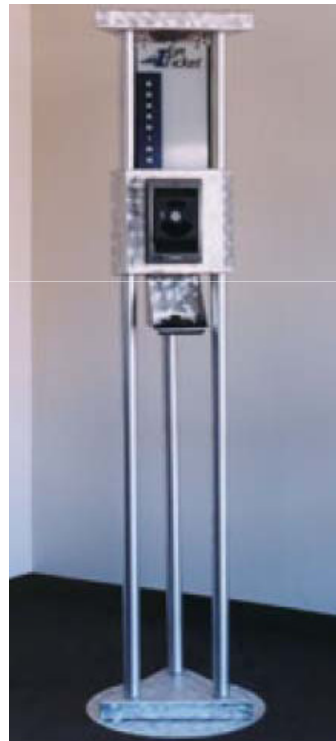
- Ein weltweit genutzter Algorithmus
 - John Daugman, University of Cambridge
- Iris nach 25 Jahren nicht unterscheidbar
- Selbst bei eineiigen Zwillingen unterschiedlich
- Keine Erkennung von Krankheiten oder Drogenkonsum möglich
- Lebenderkennung
 - Einstrahlung und Reflektion
 - Pupillenreflex
- Schnelle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



Iris Scanner: Marktsituation



Computerzugang



Kiosk System

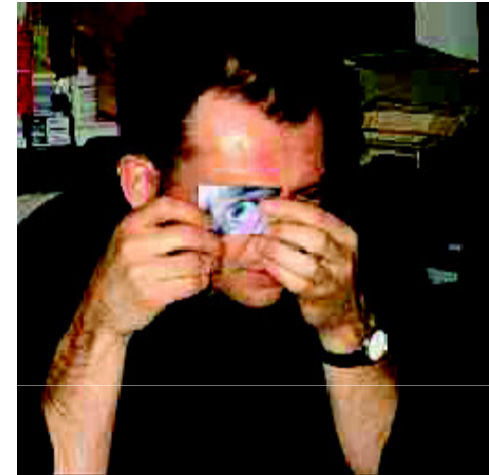


Gebäudezugang

Iris Scanner: Schwachstellen



- Überlistung mit Foto oder Inkjetausdruck
- Vorspielen einer Videosequenz
- Kontaktlinse mit gedruckter oder handgemalter Iris
- Kontaklinse 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

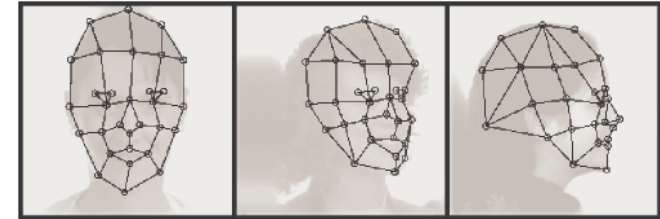


- Einleitung
- Fingerprint
- Irisscan
- Gesichtserkennung
- Gefahren
- Diskussion

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 1 %

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



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	-	--	++

- Bei Identifikation steigt die Wahrscheinlichkeit für Falscherkennung exponentiell mit Anzahl der Referenzen

Agenda



Daten sind
immer im Spiel.

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

Fiktion ?



- Video:
- Aufbringen eines fremden Fingerabdruck mit Tesafilm
- Gezielte Diskreditierung bestimmter Personen
- Falsche Schlussfolgerungen

Gefahren



- Verlust des biometrischen Merkmals
- Nicht-Ersetzbarkeit
- Fingerabdruck
 - Sicherheit
 - Eindeutig, aber nicht fälschungssicher
 - Beweislast
 - Kriminaltechnische Konsequenzen
 - Rechtliche Konsequenzen
- Technikgläubigkeit
 - Fingerabdruck von Wolfgang Schäuble
 - Einkaufen mit Fingerprint

Gefahren



- Einkaufen mit Fingerprint
- „Ökonomie der Kriminalität“
- Video:
- Einkaufen mit gefälschtem Fingerabdruck

ePass



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

- Zusätzlich zwei Fingerabdrücke
 - flach, nicht gerollt
 - als komprimierte Bilder gespeichert
 - seit November 2007

- Im kontaktlosen Chip des Passes werden darüber hinaus das Passfoto und die beiden Fingerabdrücke gespeichert

- Keine dauerhaften Kopien der Fingerbilder bei den Einwohnermeldeämtern
 - anders als zuvor von Bundesinnenminister Wolfgang Schäuble vorgeschlagen



ePass



- 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



- 13.01.2009

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

- 15.01.2009

EU-Parlament segnet Kompromissvorschlag zu biometrischen Reisepässen ab.

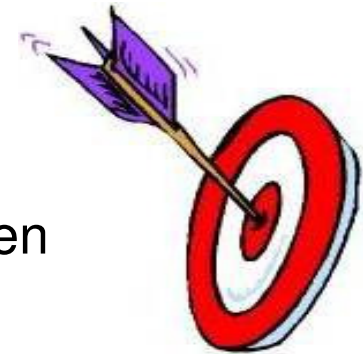
Eine Grenze für die nationalen Regierungen hat allerdings kürzlich der Europäische Gerichtshof für Menschenrechte mit seiner Entscheidung gegen die britische Regierung (Marper vs. UK) gesetzt. Darin hatte der EUGH die Speicherung von DNA-Daten und Fingerabdrücken für unverhältnismäßig und unvereinbar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

Quelle: www.heise.de

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. ■ ■ ■



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>