

■ ■ ■ Biometrie – Fluch oder Segen?



Jürgen Kühn
Senior Consultant

Frankfurt, 12.11.2014

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

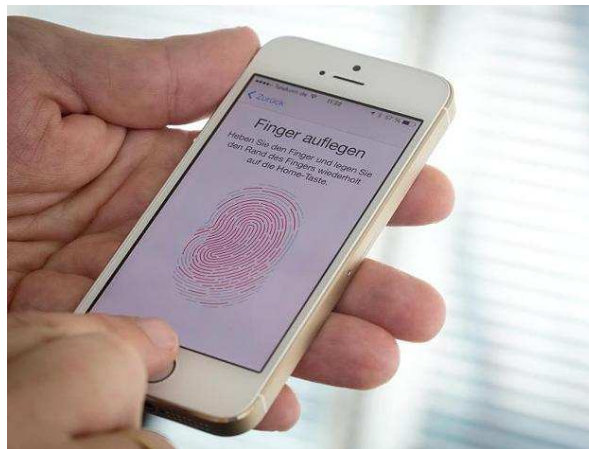
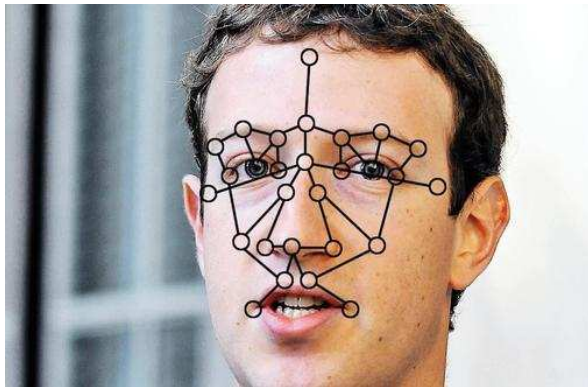
Agenda



Daten sind
immer im Spiel.

- 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 Identifikation und Authentifikation von Personen anhand von spezifischen Körpermerkmalen



Quelle: DUDEN - Das große Fremdwörterbuch

Merkmale zur biometrischen Identifikation (1)



Eigenschaften von Merkmalen zur biometrischen Identifikation

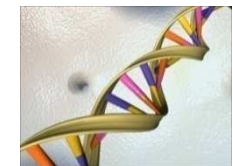
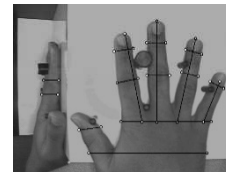
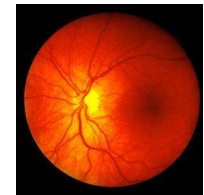
- **Universalität**
 - Merkmal ist bei jeder Person vorhanden
- **Einzigartigkeit**
 - Merkmal ist bei jeder Person anders
- **Permanenz**
 - Merkmal ändert sich über die Zeit nicht oder nur minimal
- **Erfassbarkeit**
 - Merkmal lässt sich quantitativ erheben

Merkmale zur biometrischen Identifikation (2)



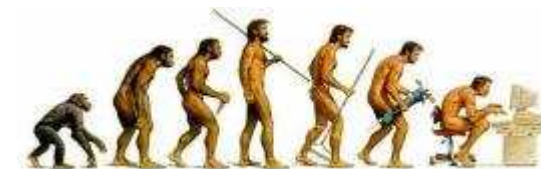
■ Physiologisches Merkmal

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



■ Verhaltensbasiertes Merkmal

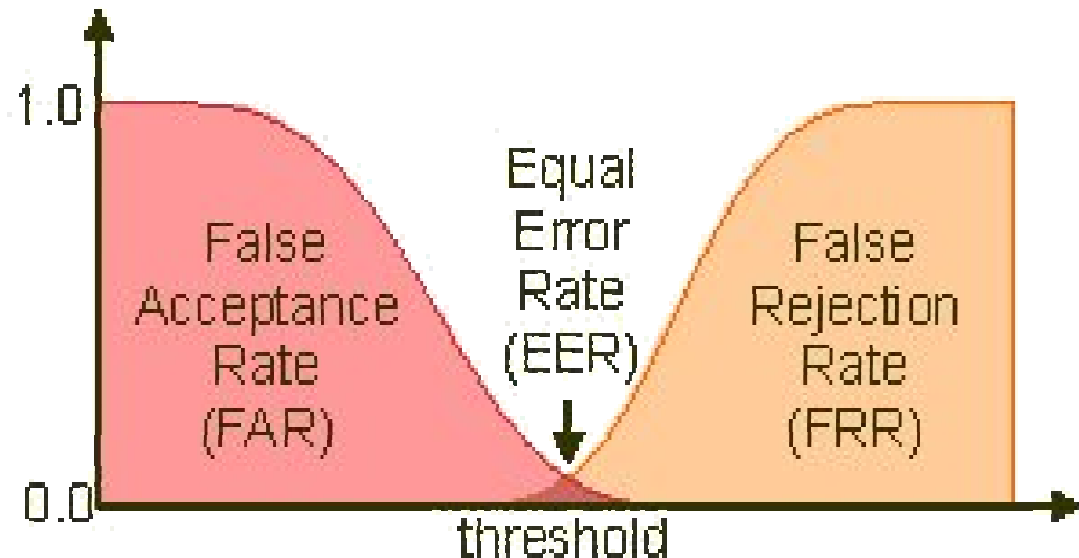
- Unterschrift (dynamisch / statisch)
- Gestik / Mimik beim Sprechen
- Gang
- Stimme / Sprechverhalten
- Tippverhalten an der Tastatur



FAR und FRR (1)



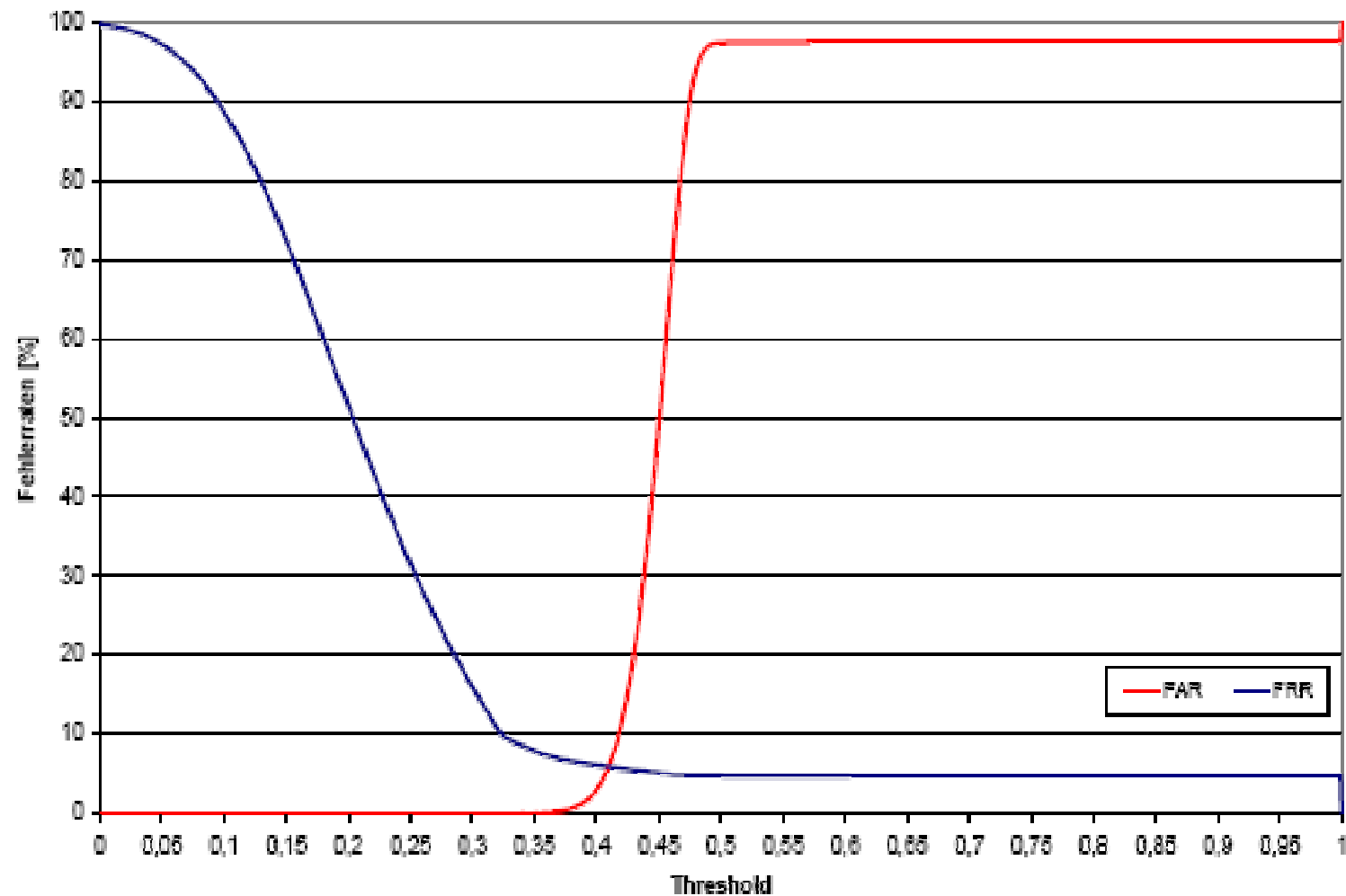
- Nur eine Wahrscheinlichkeit der Übereinstimmung
- False Acceptance Rate FAR
 - Rate der unberechtigt akzeptierten Personen
- False Rejection Rate FRR
 - Rate der unberechtigt zurückgewiesenen Personen
- Equal Error Rate ERR
 - $FAR = FRR$
- threshold bestimmt, ob das System "sicher" oder "komfortabel"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

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

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

Agenda



Daten sind
immer im Spiel.

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

Fingerprint: Funktionsweise (1)



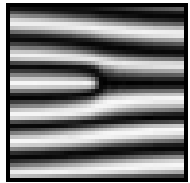
- Sensortypen
 - Optisch
 - Kapazitiv
 - Thermisch
 - Ultraschall
 - Druck
- Verfahren
 - Pattern matching über das gesamte Bild
 - Minutienbasiert
 - Verfolgen der Papillarsegmente
 - Position der Schweißporen
- 20-30 Merkmale
- Selbst bei eineiigen Zwillingen unterschiedlich
 - Bei DNA nicht



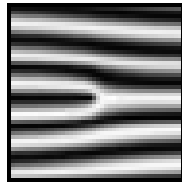
Fingerprint: Funktionsweise (2)



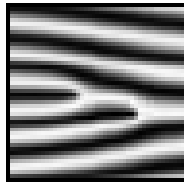
- Minutien



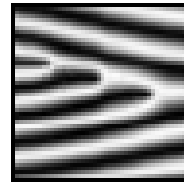
Linienende



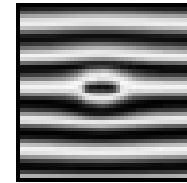
Gabelung



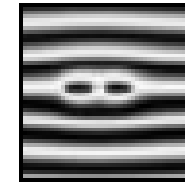
Gabelung
zweifach



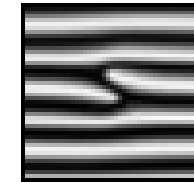
Gabelung
dreifach



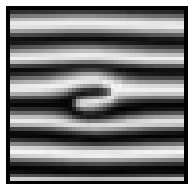
Wirbel



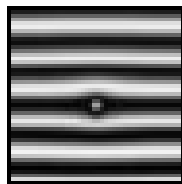
Wirbel
zweifach



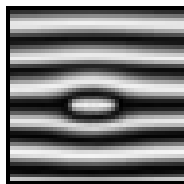
Seitliche
Berührung



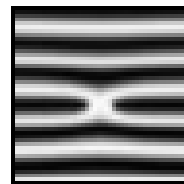
Haken



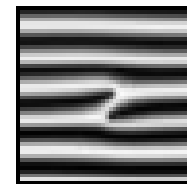
Punkt



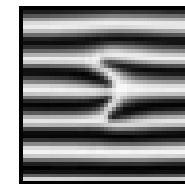
Intervall



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



Haustür



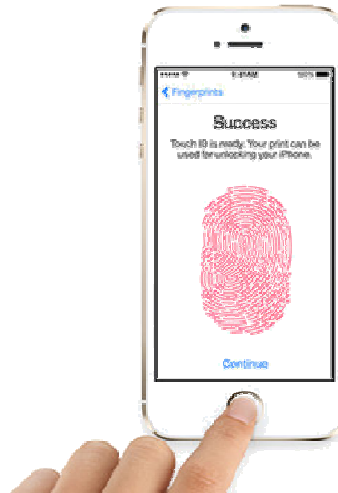
Ultraschall



integriert



integriert



optisch

Fingerprint: Schwachstellen (1)



- Latenzbildreaktivierung

- Anhauchen
- Graphitpulver
- Farbpulver

- Anfertigen einer Fingerabdruckatrappe

- Gelatine
- Holzleim

- Verwenden der Latenzabdrücke

- Graphitpulver und Tesa

- Fehlerhafte Treiber-Software

- Zugriff auf in der Windows-Registry gespeicherte Windows-Passworte
- Vorinstalliert von namhaften Notebook-Herstellern



Fingerprint: Schwachstellen (2)



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

Quelle: Kopfball

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



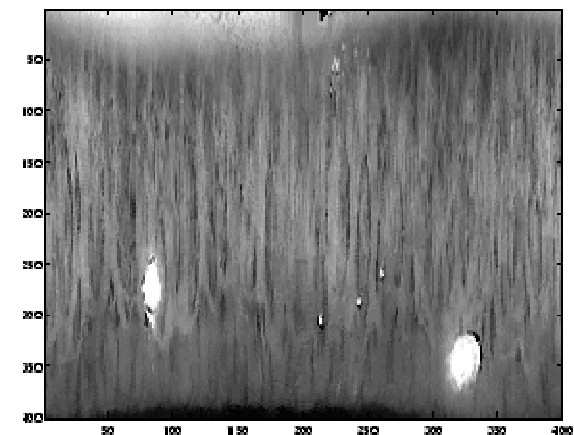
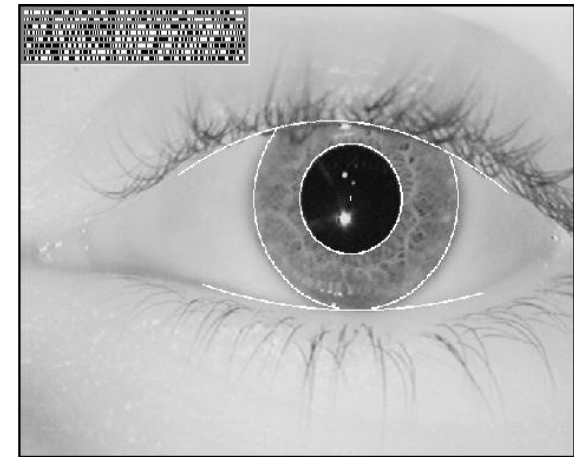
Daten sind
immer im Spiel.

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

Iris Scanner: Funktionsweise



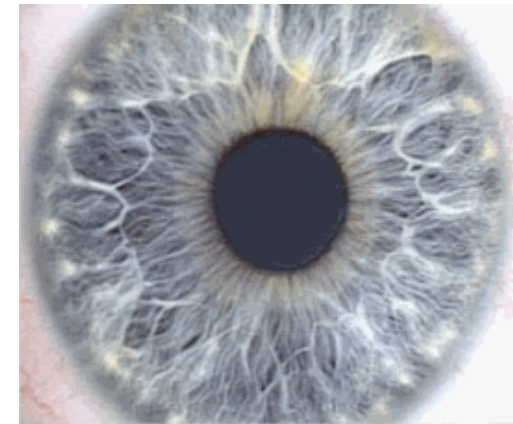
- Anstrahlen mit Infrarotlicht
- Makroaufnahme des Auges im nahen Infrarotbereich (680-850 nm)
- Extraktion der Iris
- Aufteilen der Iris in 8 kreisförmige Abschnitte
- Erkennung markanter Muster (Corona, Krypten, Fasern, Flecke, Narben, radiale Furchen, Streifen)
- Erzeugen des Iriscodes
 - Gabor Wavelet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



Iris Scanner: Funktionsweise



- Ein weltweit genutzter Algorithmus
 - John Daugman, University of Cambridge
- Schnelle Erkennung
- Gute FAR und FRR
- Lebenderkennung
 - Einstrahlung und Reflektion
 - Pupillenreflex
- Keine Erkennung von Krankheiten oder Drogenkonsum möglich
- Selbst bei eineiigen Zwillingen unterschiedlich
- Iris nach 25 Jahren nicht unterscheidbar
 - Nach Kevin Bowyer ändert sich die Fehlerrate schon nach 2 Jahren
 - Immer häufiger Folge-Scans erforderlich



Iris Scanner: Leser



Gebäudezugang



Computerzugang



eGate



Kiosk System

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



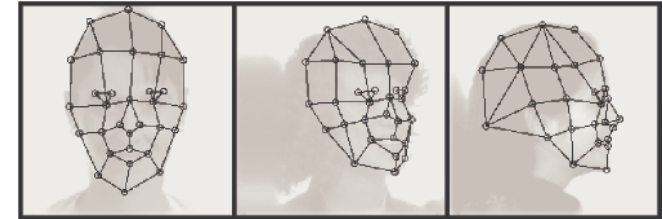
Daten sind
immer im Spiel.

- 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

-

© 2007 **trivadis**
makes IT easier.

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)

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)



Wir entdecken unseren Körper

Wieso?
Weshalb?
Warum?

Knochen sind das Gerüst unseres Körpers.

... und von dir.

Nur Zwillinge sehen sich zum Verwechseln ähnlich. Oft haben sie sogar die gleiche Art zu sprechen und sich zu bewegen.

ANNA TIBO HELEN

Ferse

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

Wunschzettel



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.

Quelle: www.heise.de

Biometrie - Fluch oder Segen?

FBI Biometrie Datenbank (1)



FBI nimmt weltgrößte Biometrie-Datenbank stückweise in Betrieb
(25.3.2011)

- Das "Next Generation Identification"-System habe die erste Phase der "operationalen Einsatzfähigkeit" erreicht
- Ersetzt das Integrated Automated Fingerprint Identification System (IAFIS) der US-Polizeibehörde
- Wird daher zunächst mit Fingerabdrücken gefüttert.
- Später sollen auch Iris-Scans, Stimmproben, Abbildungen von Handabdrücken, Tätowierungen, Narben und Gesichtsformen erfasst werden.

FBI Biometrie Datenbank (2)



- In der FBI-Niederlassung in Clarksburg im US-Bundesstaat Virginia werden derzeit täglich durchschnittlich rund 168.000 Fingerabdrücke analysiert und identifiziert.
- Das System soll künftig 18.000 Strafverfolgungsbehörden rund um die Uhr eine automatisierte Suche nach Fingerabdrücken, einen Echtzeit-Abgleich und einen zugehörigen Informationsaustausch erlauben. Ermittler vor Ort sollen künftig auch mit Hand-Scannern ausgerüstet werden.
- Das Department of Homeland Security (DHS) hat parallel ein eigenes System zur Erfassung von Fingerabdrücken und Iris-Scans von Einreisenden in die USA etwa an Flughäfen aufgebaut.
- Für den US-Bürgerrechtler Barry Steinhardt von der Datenschutzorganisation Privacy International steht damit außer Frage, dass biometrische Systeme eine wichtige Komponente künftiger staatlicher Überwachungsprojekte bilden werden. Er warnt davor, dass durch deren Abgleichmöglichkeiten eine "Always on"-Überwachungsgesellschaft möglich werde. Der kalifornische Zukunftsforscher Paul Saffo warnt in diesem Zusammenhang davor, dass biometrische Merkmale anders als etwas Kreditkartennummern einem Menschen sein Leben lang anhafteten. Fehler in staatlichen Datenbanken könnten daher gravierende Folgen haben.

Falsche Analyse (1)



Tödliche Vertuschung beim FBI (19.4.2012)

- US-Regierung kannte seit den 90er-Jahren erhebliche Fehlerquellen in Untersuchungslaboren der Bundespolizei FBI
- Die Ergebnisse wurden viele Jahre zurückgehalten
- Eklatante Fehler bei der Analyse von Haarproben und Hautresten in Mord- und Tötungsdelikten
- Hunderte Fälle von Justizirrtümern und ungerechtfertigten Strafen
- Unschuldige blieben hinter Gittern oder wurden hingerichtet

Quelle: <http://www.derwesten.de/panorama/hunderte-justizirrtuemer-toedliche-vertuschung-beim-fbi-id6569273.html>

Falsche Analyse (2)



- In den 90er-Jahren groß angelegte Untersuchung
 - Das Justizministerium ließ 6000 Fälle nachträglich rekonstruieren
 - Die Untersuchung dauerte neun Jahre
- Die Ergebnisse wurden 2004 aber weder an die zum Teil seit vielen Jahren zu Unrecht einsitzenden Häftlinge noch an deren Anwälte weitergegeben
- Allein die beteiligten Staatsanwälte wurden informiert, behielten die teils entlastenden Erkenntnisse aber weitgehend für sich
- Zu Unrecht Verurteilte wurden nicht rehabilitiert

Quelle: <http://www.derwesten.de/panorama/hunderte-justizirrtuemer-toedliche-vertuschung-beim-fbi-id6569273.html>

Falsche Analyse (3)



- Der 17jährige Santae Tribble wurde eines Mordes für schuldig befunden, obwohl mehrere Zeugen unter Eid aussagten, dass Tribble zur Tatzeit bei ihnen gewesen sei
- Kernstück der Beweisführung der Staatsanwaltschaft waren Haarproben, die Tribble zugeordnet wurden
- Wie sich bei den internen Prüfungen herausstellte, handelte es sich bei den FBI-Beweisgegenständen in Wahrheit um Hundehaare
- Ein Kriminaltechniker hat offensichtlich gerade bei Haaranalysen mehrfach fatale Fehler begangen

Quelle: <http://www.derwesten.de/panorama/hunderte-justizirrtuemer-toedliche-vertuschung-beim-fbi-id6569273.html>

Falsche Analyse (4)



- Verschlussache-Report des damaligen FBI-Generalinspektors Michael Bromwich von 1997
- "FBI-Experten sind mehrfach zu „unwissenschaftlichen Schlussfolgerungen gekommen“, die für die Beschuldigten von großem Nachteil waren."
 - Bombenattentat von Oklahoma 1995
 - Mordprozess gegen den früheren Footballstar O.J. Simpson
 - Erste Anschläge auf das World Trade Center in New York 1993
- Auch dieser Bericht verschwand in den Aktenbergen

Quelle: <http://www.derwesten.de/panorama/hunderte-justizirrtuemer-toedliche-vertuschung-beim-fbi-id6569273.html>

Falsche Analyse (5)



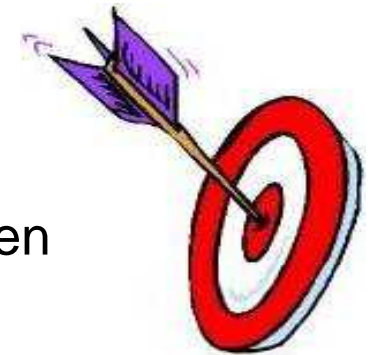
- Nach den Attentaten vom 11. September 2001 änderten sich sicherheitspolitisch die Prioritäten in den USA, das Thema geriet ins Abseits
- Mehrere der damals Verantwortlichen sind inzwischen verstorben oder nicht mehr in öffentlichen Ämtern
- Aufklärung verspricht sich die „Washington Post“ von Janet Reno, damals Generalstaatsanwältin, derzeit erkrankt
- Wie viele heute noch in Haft sitzende Männer und Frauen Opfer der Vertuschungen sind, bleibt vorläufig offen
- Das Justizministerium weigert sich, die Namen jener Menschen herauszugeben, denen durch Experten des FBI Unrecht geschah

Quelle: <http://www.derwesten.de/panorama/hunderte-justizirrtuemer-toedliche-vertuschung-beim-fbi-id6569273.html>

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!



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>

Notizen behalten



- Siehe Notizen