Biometrische Zugangskontrolle

Christoph Busch

Hochschule Darmstadt - CRISP

2017-03-16

da/sec
BIOMETRICS AND INTERNET-SECURITY
RESEARCH GROUP

LOEWE

HESSEN

Biometric Characteristic

Biometric activities

- Convener of the Working Group 3 on Biometric Data Interchange Formats in ISO/IEC JTC1 SC37
- Board-member European Association for Biometrics
- Chair of the TeleTrusT working group on Biometrics
- Co-Chair of the Norsk Biometri Forum

Recent projects related to Biometrics

- Hochschule Darmstadt:
  - LOEWE/BMBF CRISP http://www.crisp-da.de/
  - LOEWE BioMobile http://www.christoph-busch.de/projects-biomobile.html
- NorwegianBiometricsLab@NTNU:
  - EU-FP7 INGRESS http://www.ingress-project.eu
  - EU-FP7 ORIGINS http://www.origins-project.eu
  - EU-FP7 PIDaaS http://www.pidaas.eu
  - IKTPLUSS SWAN https://www.ntnu.edu/aimt/swan

CRISP
Center for Research in Security and Privacy

Kontext IT-Sicherheit

Darmstadt ist das Security Valley in Deutschland

- 1999
  Center for Applied Security Technology (CAST)

- 2002
  Darmstädter Zentrum für IT−Sicherheit (DZI)

- 2008
  Center for Advanced Security Research Darmstadt (CASED)

- 2011
  European Center for Security and Privacy by Design (EC-SPRIDE)

- 2015
  Center for Research in Security and Privacy (CRISP)

Warum Biometrie als Authentisierungs Faktor?

Zugangskontrolle

Eine Authentisierung kann erreicht werden:

- durch Wissen:
  Password, PIN, ...

Zugangskontrolle

Statistik basierend auf 32 Millionen Passworten

- 20% sind Namen und triviale Passworte

Rank	Password	Number of Users with Password (absolute)
1	123456	290731
2	12345	79078
3	123456789	76790
4	Password	61958
5	iloveyou	51622

Source: Imperva

Zugangskontrolle

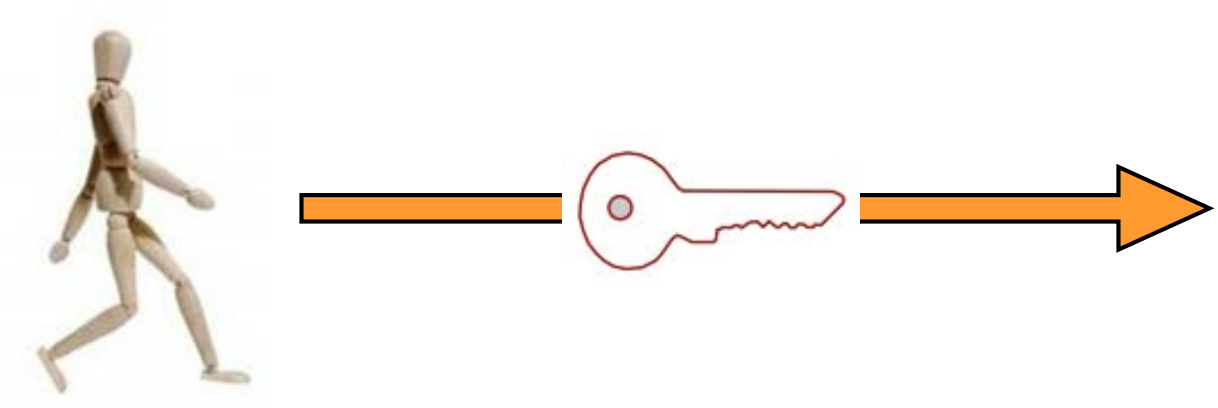
Eine Authentisierung kann erreicht werden:

- durch Wissen:
  Password, PIN, ...
- durch Besitz:
  SmartCard, USB-token, key

Zugangskontrolle

Traditionell etablieren wir zwischen

- natürlichen Personen
- und Objekten
- einen Token (d.h. einen Schlüssel) zur Zugangskontrolle



Zugangskontrolle

Aber in der Realität haben wir

- nicht nur einen
  - sondern viele Schlüssel
  - und Zugang zu vielen Türen

Zugangskontrolle

Eine Authentisierung kann erreicht werden:

- durch Wissen:
  Password, PIN, ...

- durch Besitz:
  SmartCard, USB-token, key

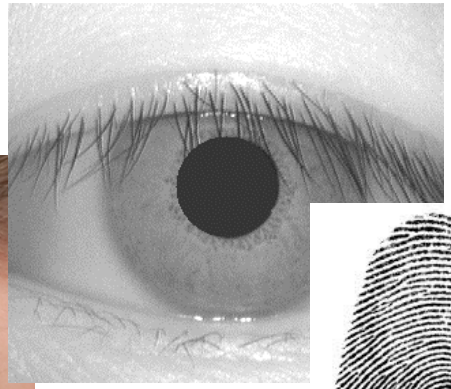
- durch Biometrie: Charakteristik des menschl. Körpers

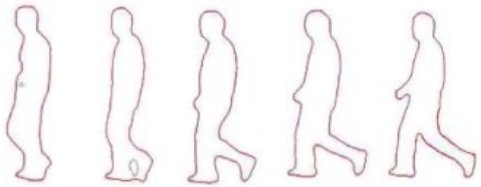
Wissen oder Besitz kann man leicht
verlieren,vergessen oder weitergeben,
biometrische Charakteristika nicht ohne weiteres.

Definition

- International Organization for Standardization definiert:
  - **Biometrics**:
    "*automated recognition of individuals based on their behavioural and biological characteristics* "
  - Anmerkung: behavioural bezieht sich auf die Funktion des Körpers
  - biological / anatomical bezieht sich auf die Struktur des Körpers





Wie funktionieren biometrische Systeme?

Beispiel: Fingerabdruck-Erkennung

Analoge/digital Repräsentation der Papillarleisten

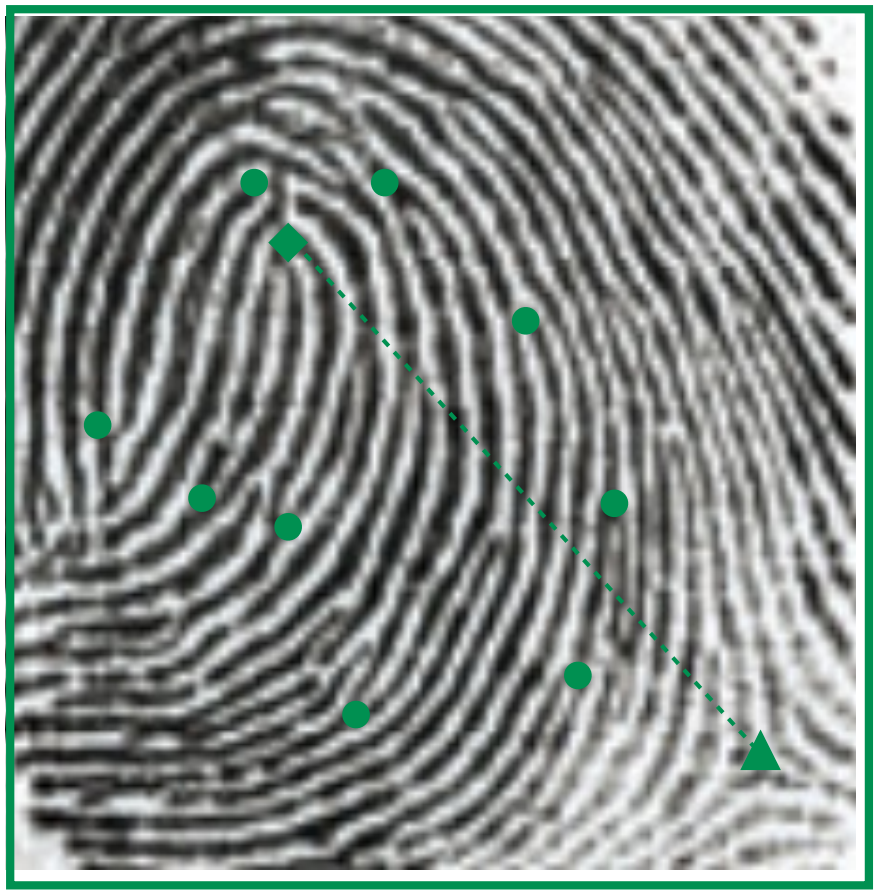
- Landmarken im Fingerbild: Minutien

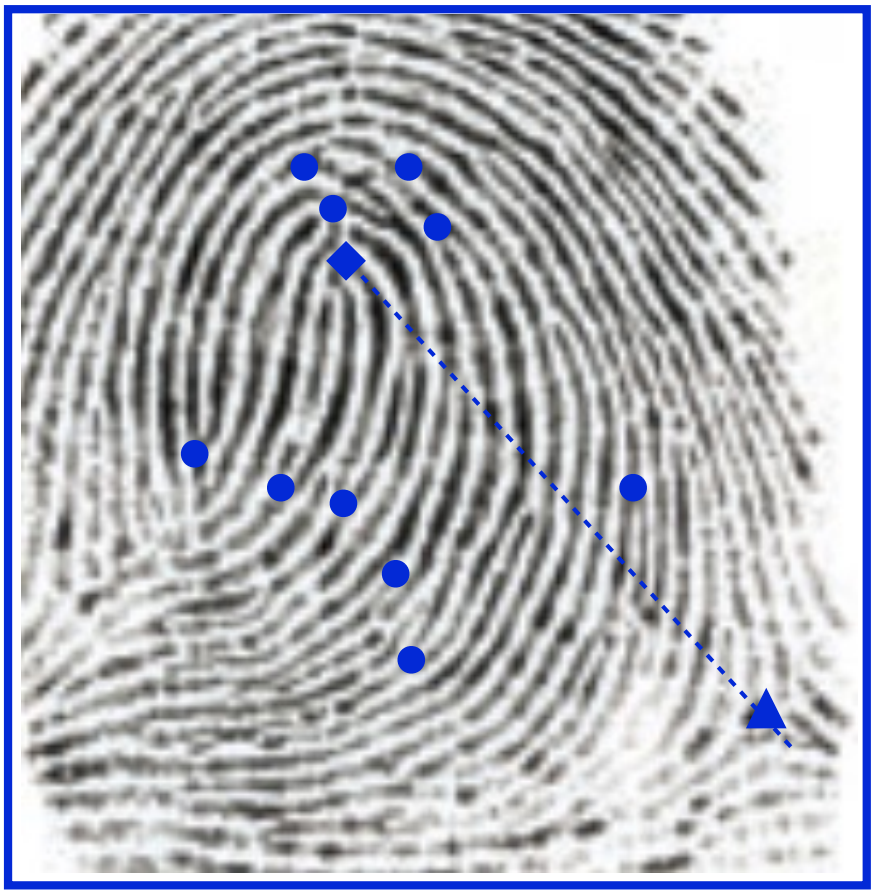
Beispiel: Fingerabdruck-Erkennung

Vergleich des Reference Image
mit dem Probe Image

Beispiel: Fingerabdruck-Erkennung

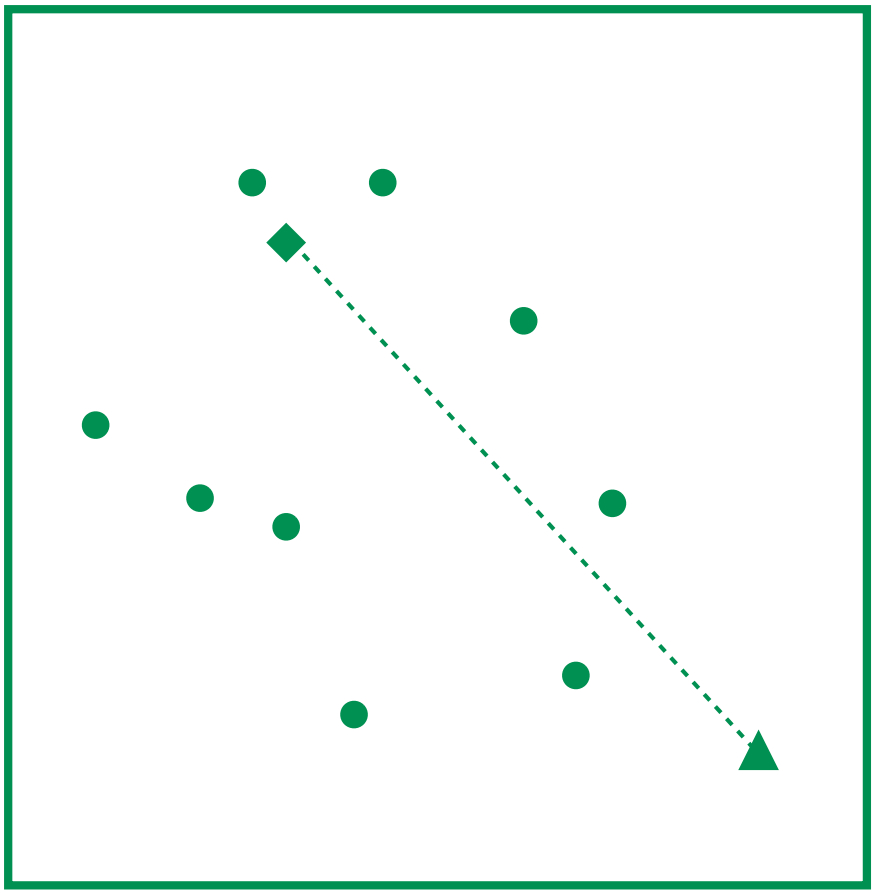
Vergleich des Reference Image
mit dem Probe Image

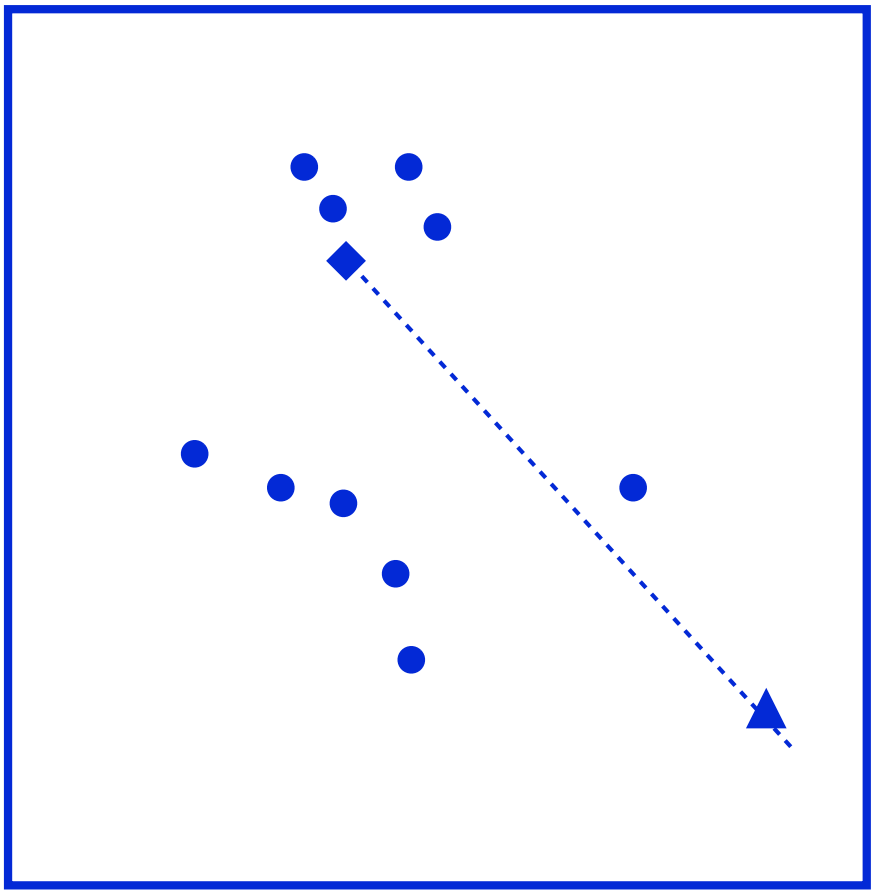




Beispiel: Fingerabdruck-Erkennung

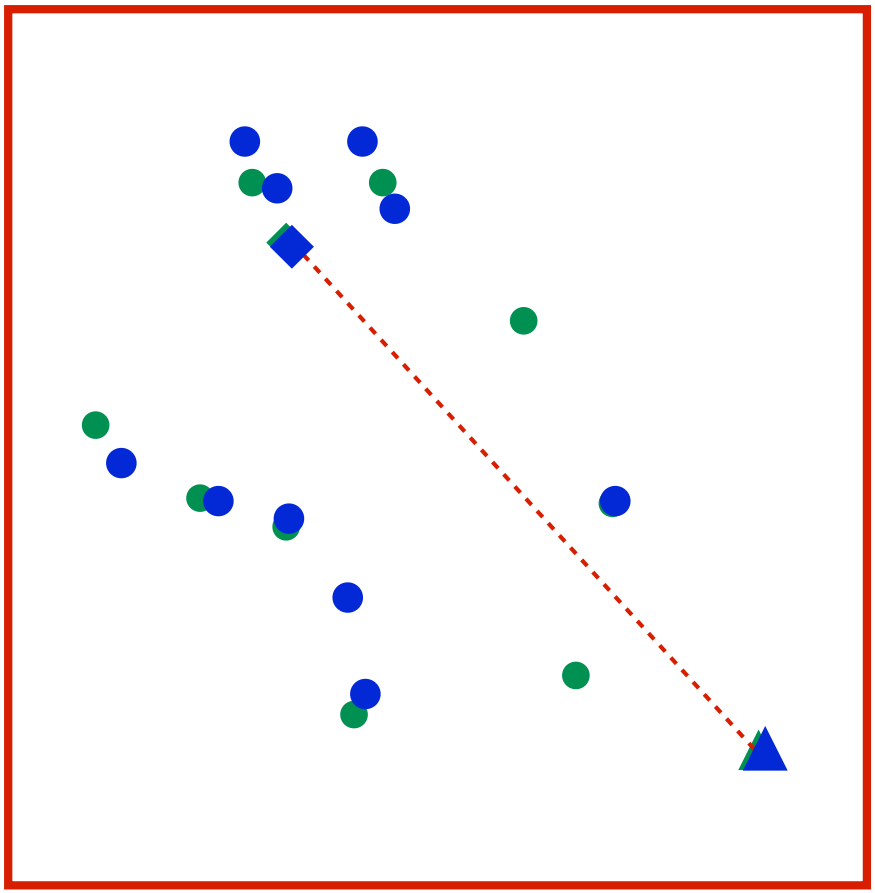
Vergleich des Reference Merkmalsvektors
mit dem Probe Merkmalsvektors





Beispiel: Fingerabdruck-Erkennung

Vergleich des Reference image
mit dem Probe image



Generische Funktionsweise

Die biometrische Charakteristik des Benutzers wird aufgezeichnet und gespeichert (Enrolment)

- Der Benutzer wird dem Rechner quasi vorgestellt.

Beim Authentisierungsversuch wird die Charakteristik wiederum aufgenommen und mit der gespeicherten Referenz verglichen.

- Wird ein Schwellwert überschritten, gilt der Benutzer als authentisiert.

Währenddessen laufen Prozesse zur Erkennung von Fälschungen ab, um Angriffe auszuschließen.

- (so genannte „Lebend-Erkennung“)

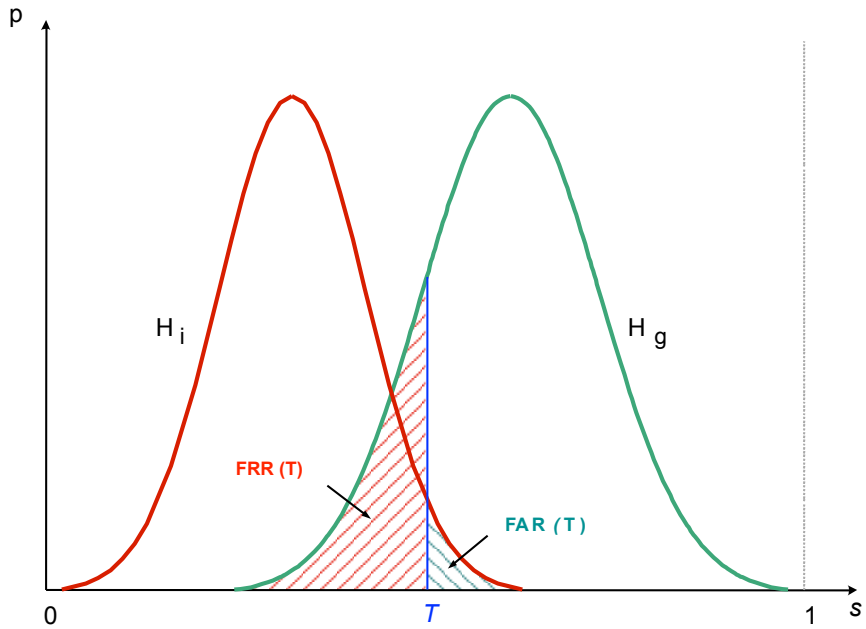
Erkennungsleistung

Falsch-Azeptanz-Rate (FAR)

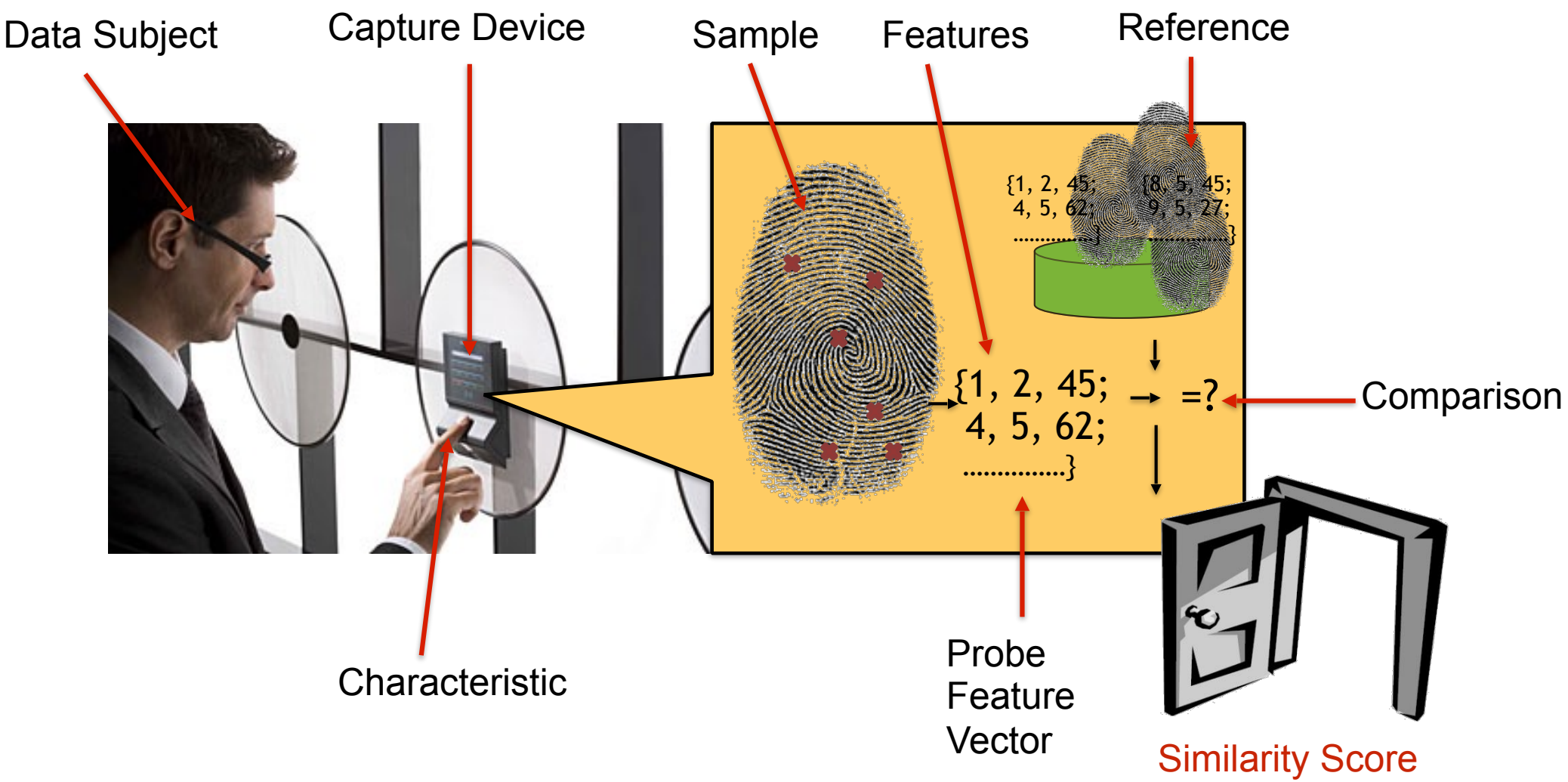
- Gibt in Prozent an, bei welchem Anteil von Versuchen eine Falsch-Erkennung erfolgte, d.h. eine falsche Identität zugewiesen wurde

Falsch-Rückweisungs-Rate (FRR)

- Gibt an, welcher prozentuale Anteil von Versuchen von berechtigten Benutzern fälschlicherweise abgewiesen wurde



Workflow in einem Biometric System



Biometrie in der Zugangskontrolle

Sollte es

- biometrische Zugangskontrolle an jeder Tür geben?

- Kosten-Faktor Sensoren?
- Wo Referenzen hinterlegen?

Smartphone Based Access Control

Es wird nicht lange dauern

- bis NFC enabled Smartphones mit den meisten Türen interagieren

Das Mobiltelefon
ist eine Bedrohung!

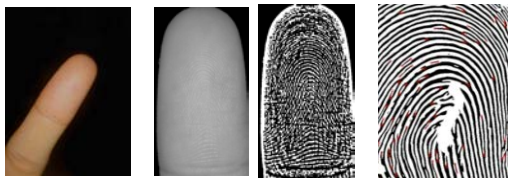
Zitat: Verband der Schlüssel-Produzenten (vom 07.12.2011)

Smartphone - Zugangskontrolle

Foreground authentication (Nutzer Interaktion)

- Integrierte Sensoren seit Apple iPhone 5S
- Kamera als Sensor
  - Fingerabdruckerkennung
  - Gesichtserkennung
  - Augenerkennung

Image Source: Apple 2013



Background authentication (Beobachtung des Nutzers)

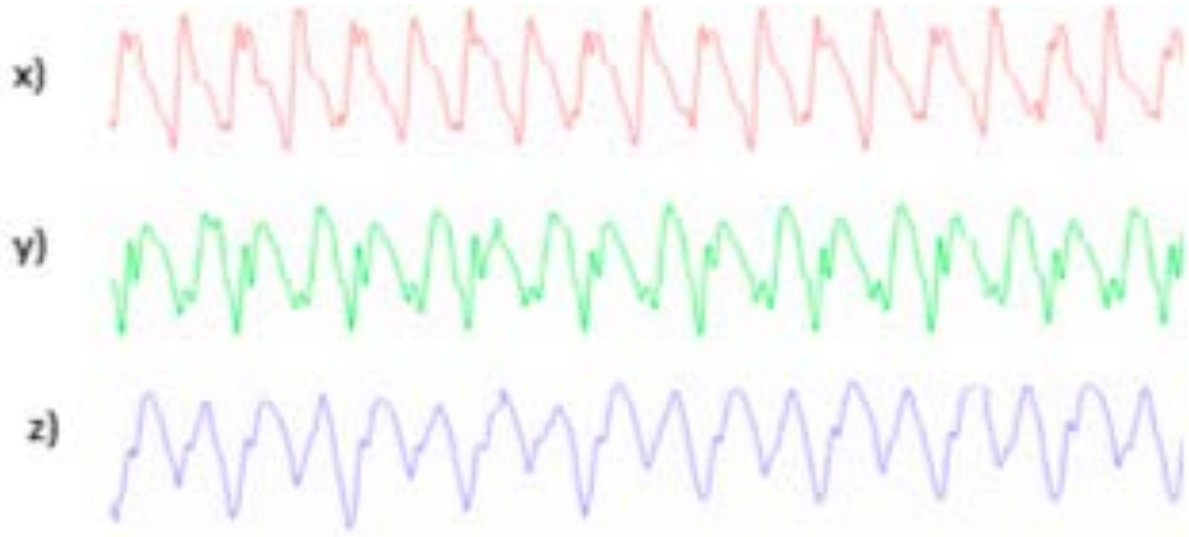
- Mikrophon
  - Sprechererkennung
- Accelerometer - Beschleunigungssensor
  - Gangerkennung
- nebenläufig ohne Beeinträchtigung

Gangerkennung

Biometrische Gangerkennung

Erlaubt eine nebenläufige Authentisierung durch Anlayse des Schrittmusters

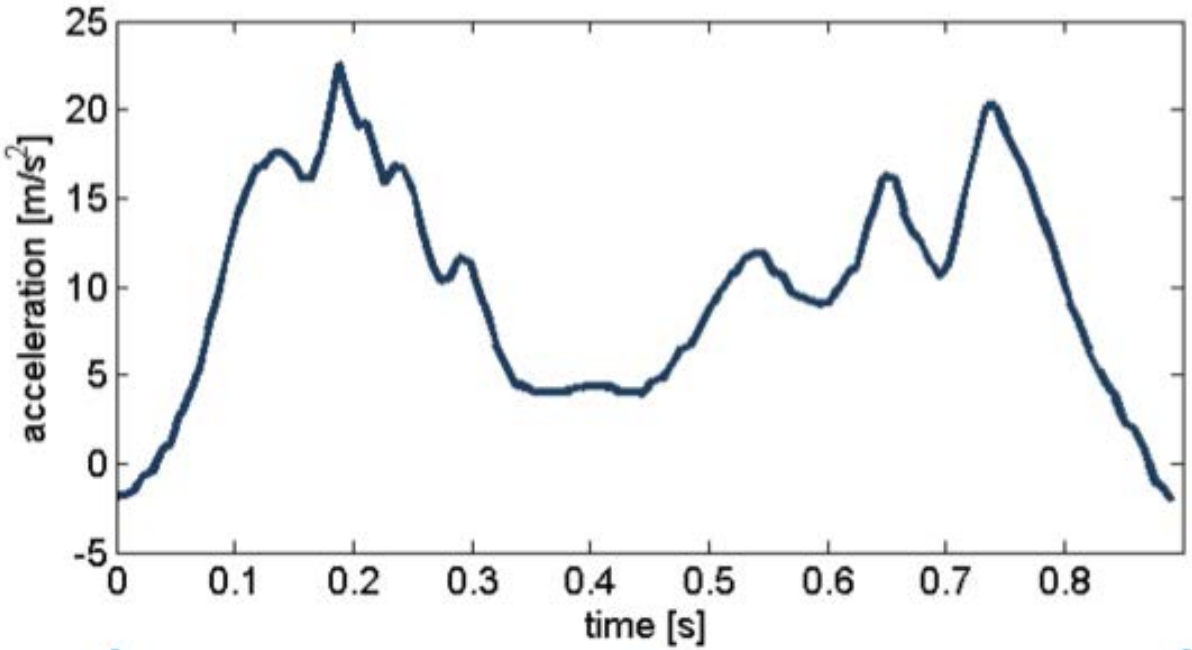
- Nutzung von Beschleunigungs-Sensor - die ohnehin im Mobilgerät verbaut sind
  - Die meisten Smartphones enthalten einen Accelerometer
  - Beschleunigung in drei Richtungen

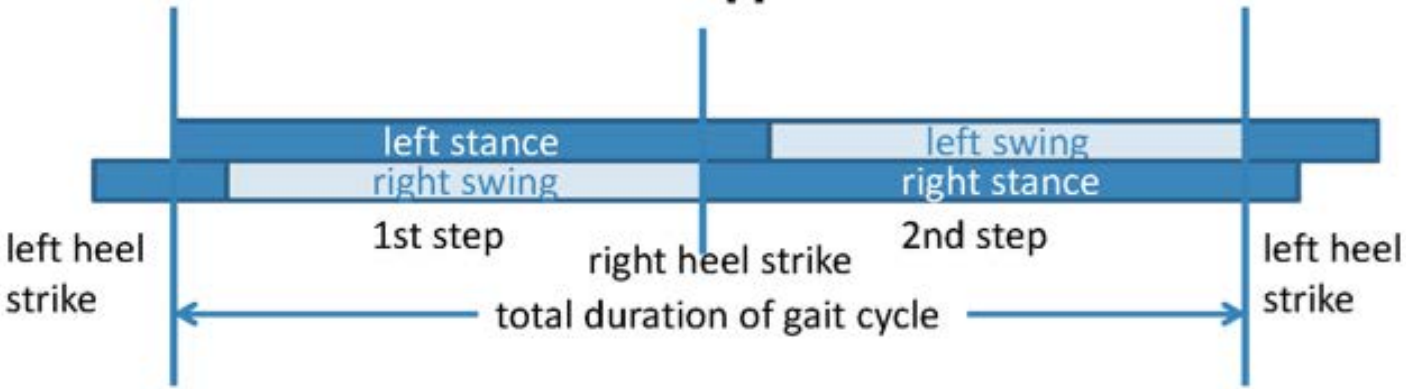


Biometrische Gangerkennung

Aufzeichnung des Schrittmusters

- Periodisches Muster

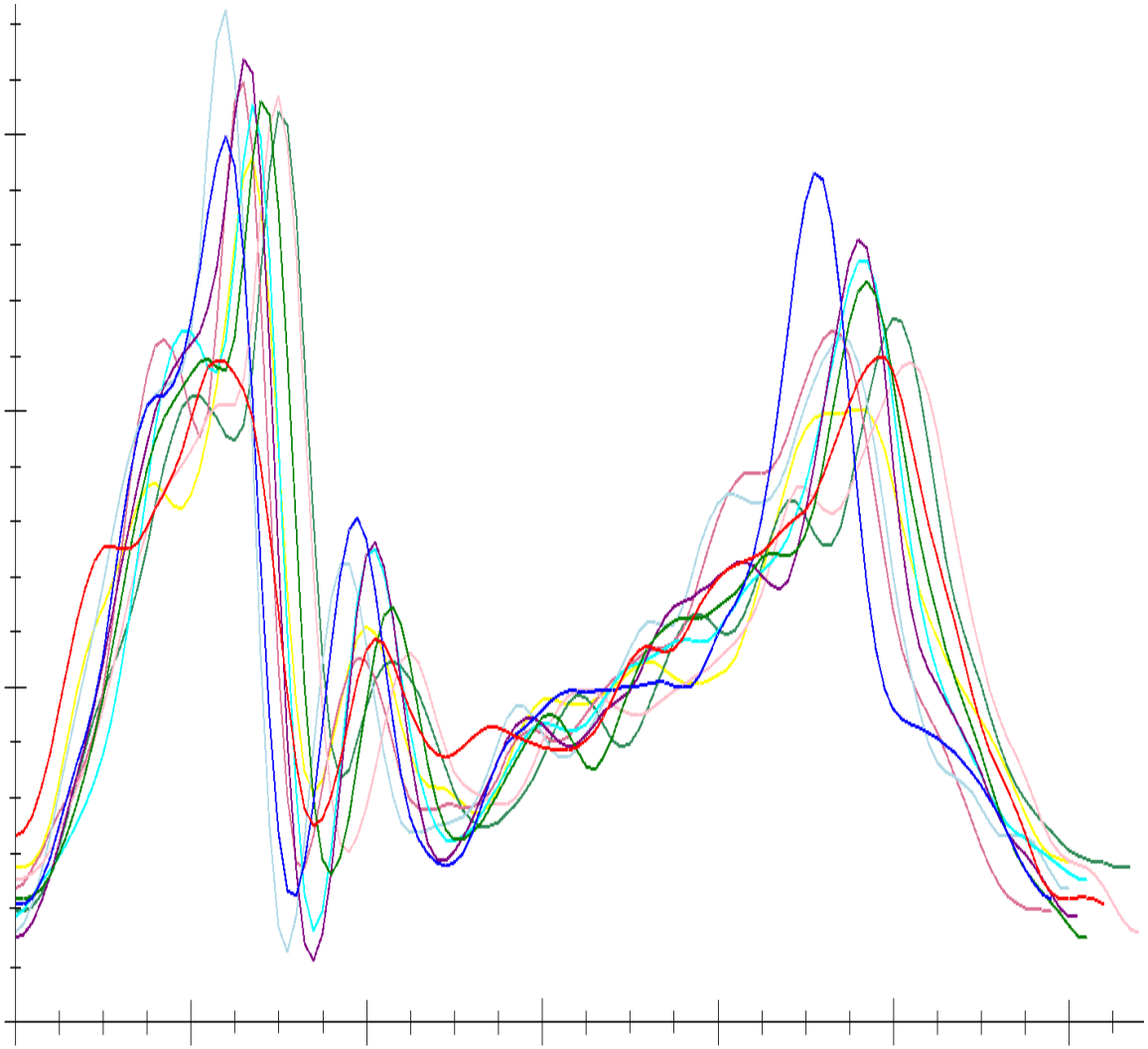




Gangerkennung - Zuverlässigkeit?

Niedrige Intra-Class Varianz

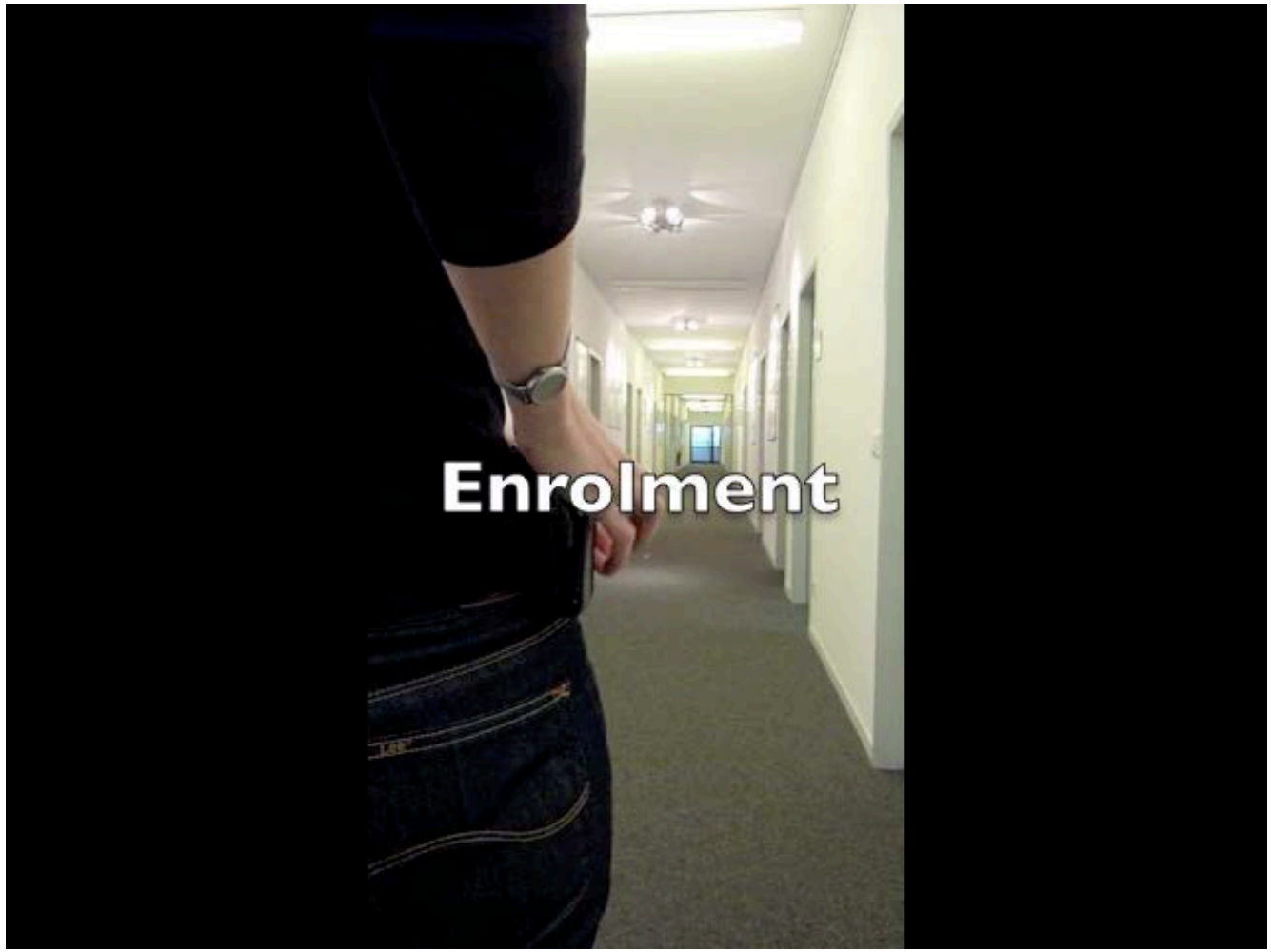
- Hohe inter-class Varianz



Authentisierung an Smartphones

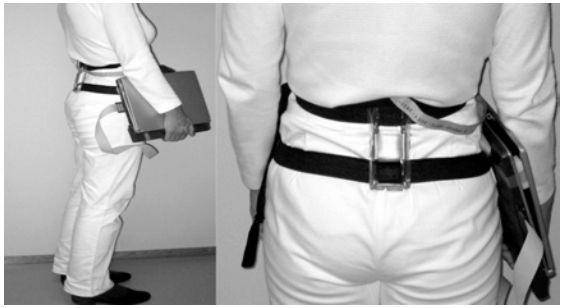
Modular Biometric Authentication Service System

- MBASSy - Film



Ergebnisse

- Alle Veröffentlichungen, die Trainings- und Testdaten von unterschiedlichen Tagen verwenden



Veröffentlichung	Sensor	Sensor-position	Anzahl Personen	Bestes Ergebnis [%]
Ailisto [4], 2005	dediziert	Rücken	36	6,4 (EER)
Rong [123], 2007	dediziert	Rücken	21	5,6 (EER)
Pan [61], 2009	Wiimote	Hüfte	30	70,1 (GMR)
Sprager [130], 2009	Handy	Hüfte	6	92,9 (CCR)
Gafurov [46], 2010	dediziert	Knöchel	10	59,0 (GMR)
Nickel (CASED)	Handy	Hüfte	48	6,1 (EER)

Biometrische Sprechererkennung

Projekt BioMobile II

Biometrische Sprechererkennung

Bietet sowohl eine nebenläufige als auch explizite Authentisierungsmethode

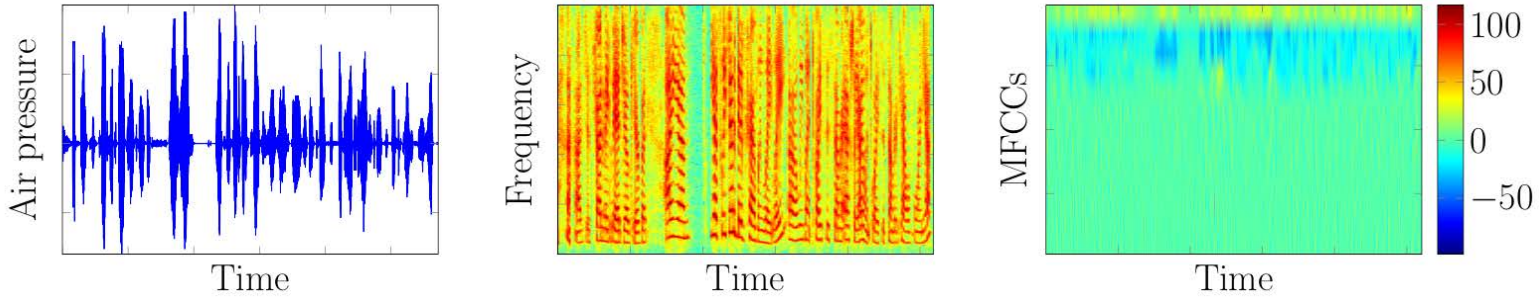
- Verwendung des eingebauten Mikrophons
  - Kopplung mit Challenge Response bei Transaktionen




Biometric Speaker Recognition

Stand der Technik

- Psychoacoustic spectrum analysis
  - 60 Mel-Frequency Cepstrum Coefficients (MFCCs)



- |
  - 2048 × 60 free parameter per sample
- Total Variability Analysis: intermediate-sized vectors
  - 400-dimensional identity vectors (i-vector)

Zusammenfassung

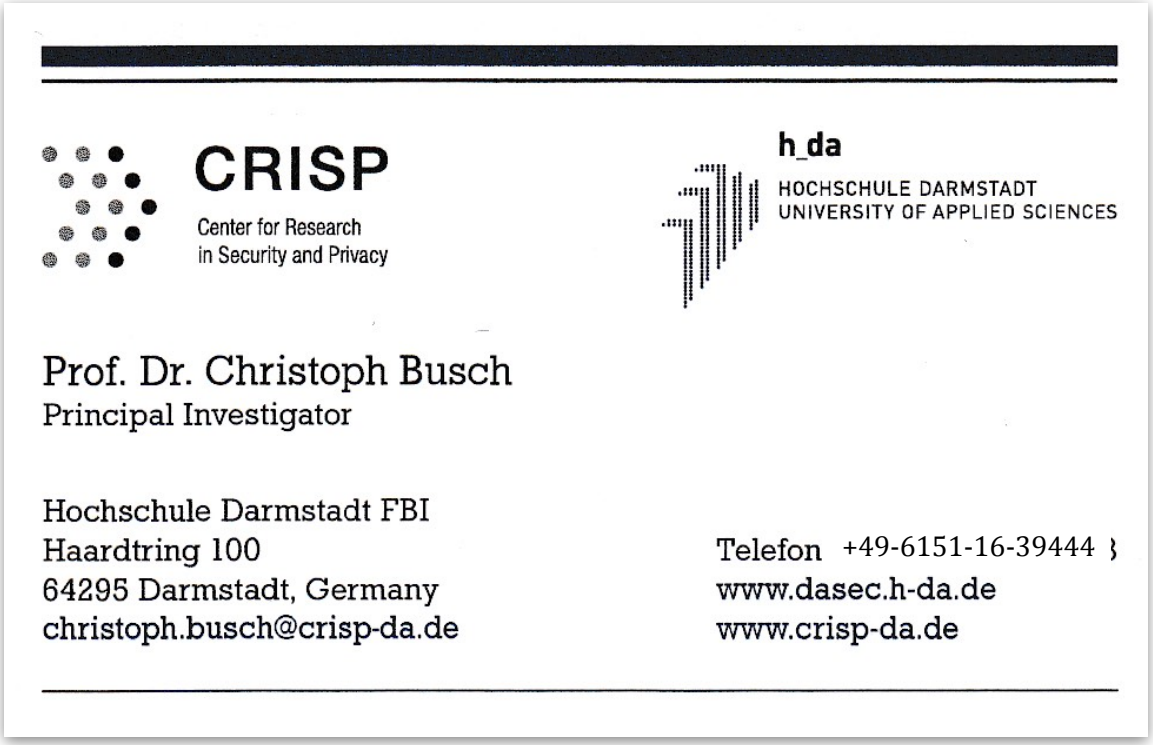
- Biometrie kann zur Steigerung der Sicherheit eingesetzt werden
- Smartphones werden Schlüssel ablösen
  - Türen können sich ohne Interaktion öffnen, wenn das berechtigte Smartphone in der Nähe ist
- Biometrische Authentisierung am Smartphone
  - komfortabel
  - ohne neue Sensoren und damit ohne Kosten möglich
- Gangerkennung und Sprechererkennung zeigen eine gute Erkennungsleistung

References

Web

- da/sec biometric research group
  https://www.dasec.h-da.de/
- European Association for Biometrics
  http://www.eab.org
- TeleTrusT working group on Biometrics
  http://www.christoph-busch.de/about-ag-biometrie.html
- Center for Research in Security and Privacy (CRSIP)
  https://www.crisp-da.de/
- Competence Center for Applied Security Technology (CAST)
  https://www.cast-forum.de

Kontakt


CRISP
Center for Research
in Security and Privacy
h_da
HOCHSCHULE DARMSTADT
UNIVERSITY OF APPLIED SCIENCES
Prof. Dr. Christoph Busch
Principal Investigator
Hochschule Darmstadt FBI
Haardtring 100
64295 Darmstadt, Germany
christoph.busch@crisp-da.de
Telefon +49-6151-16-39444
www.dasec.h-da.de
www.crisp-da.de