

Anwendungsorientierte Forschung in CASED - Biometrische Absicherung von Smartphones

Christoph Busch

Hochschule Darmstadt - CASED / Gjøvik University College
<http://www.christoph-busch.de/>

26. Juni 2012

Gjøvik University College

- once you drink the water of Mjøsa - you will stay ...



Agenda

- Einführung
- CAsED
- Zugangskontrolle
- Biometrische Authentisierung
- NFC und Smartphones
- Gangerkennung
- Komfort und Authentisierung

Einführung

Dieser Vortrag behandelt:

- „**Biometrische** Absicherung von Smartphones“

Was ist Biometrie?

- International Organization for Standardization:



- ▶ Biometrics (06/2004):

*“Automated recognition of individuals
based on their behavioral and biological characteristics.”*

Einführung

Was ist Biometrie?

- Ein dynamisches Mood Board



Eigentlich hat dieser Vortrag
noch einen zweiten Titel

Verantwortung

Verantwortung

Eintritt in umfassende Verantwortung

- Ein Ereignis in 2003:

18. November 2003

Prof. Dr. Maria Overbeck-Larisch zur Präsidentin der FH Darmstadt gewählt

Die Wahlversammlung der Fachhochschule Darmstadt hat am heutigen Nachmittag Prof. Dr. Maria Overbeck-Larisch (55) für sechs Jahre zur Präsidentin der Hochschule gewählt. Ihre Amtszeit beginnt am 1. März 2004 und endet Ende Februar 2010.



Anwendungsorientierte Forschung im CASED

IT-Security made in Darmstadt



CASED – Center for Advanced Security Research Darmstadt



LOEWE – Landes-Offensive zur Entwicklung Wissenschaftlich-ökonomischer Exzellenz



2008 bis 2014: € 410 Mio

8 LOEWE Zentren

16 LOEWE Schwerpunkte

60 Projekte mit KMU

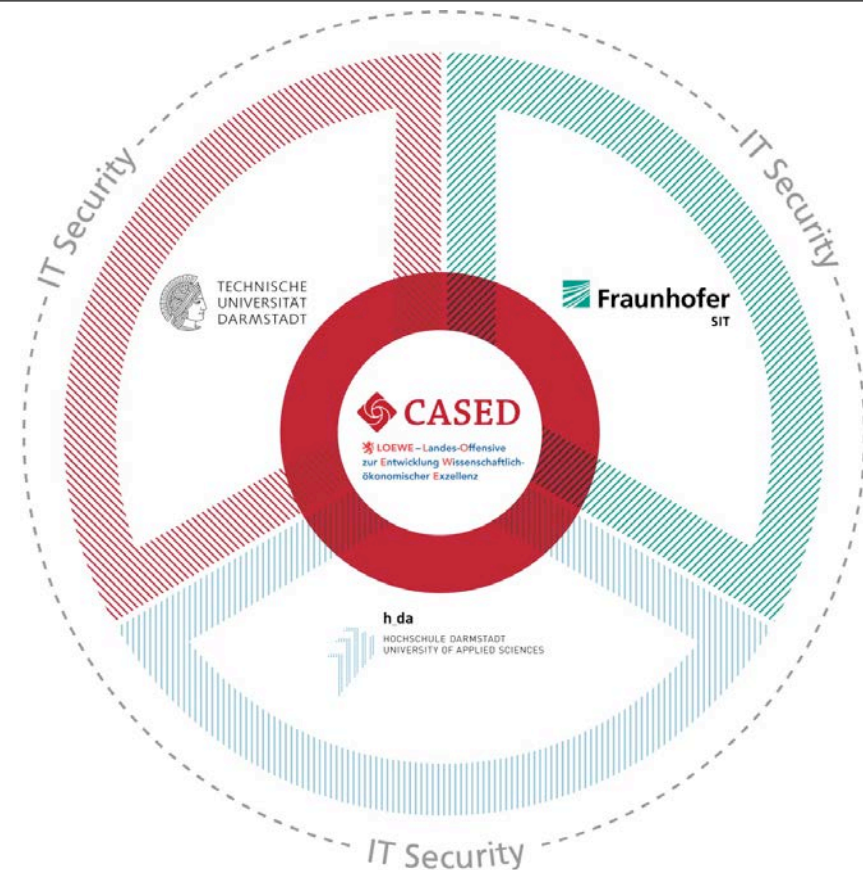
▪ **CAGED** <http://www.cased.de/>

▪ Mornewegstraße 32

▪ 64293 Darmstadt



Source: Google



LOEWE – Landes-Offensive
zur Entwicklung **Wissenschaftlich-ökonomischer Exzellenz**

Principal Investigators in CASED



▪ Technische Universität Darmstadt

- Fachbereich Informatik: 18 Professorinnen und Professoren
- Fachbereich Physik: 2 Professoren
- Fachbereich Maschinenbau: 1 Professor
- Fachbereich Elektrotechnik und Informationstechnik: 1 Professor
- Fachbereich Rechts- und Wirtschaftswissenschaften: 1 Professor
- Unterauftrag an die Universität Kassel: 1 Professor

▪ Hochschule Darmstadt

- Fachbereich Media: 1 Professor (Christoph Busch)
- Fachbereich Informatik: 1 Professor (Harald Baier)
2 assoziierte PI
(M. Braun, M. Massoth)
1 Stelle in Besetzung
(N.N.)



Harald Baier
Internet-Sicherheit



Michael Braun
Theoretische Informatik,
IT-Sicherheit,
Codierungstheorie

Arbeitsbereiche



Sichere
Daten



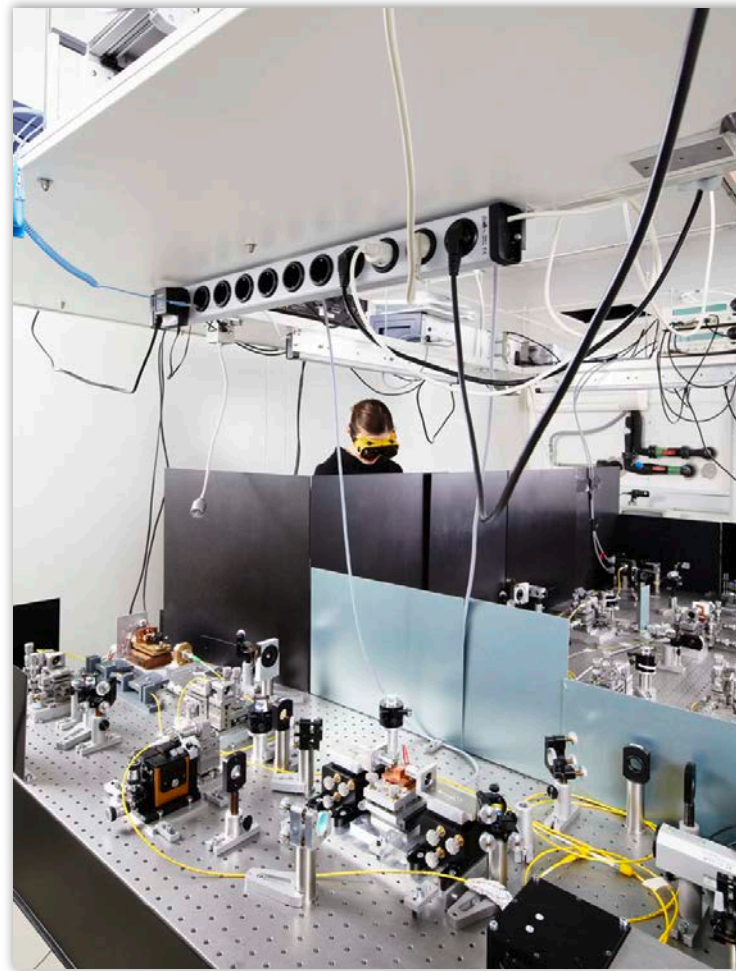
Sichere
Dinge



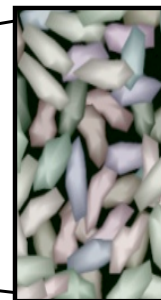
Sichere
Dienste



Beispiel: Post-Quantum Cryptography



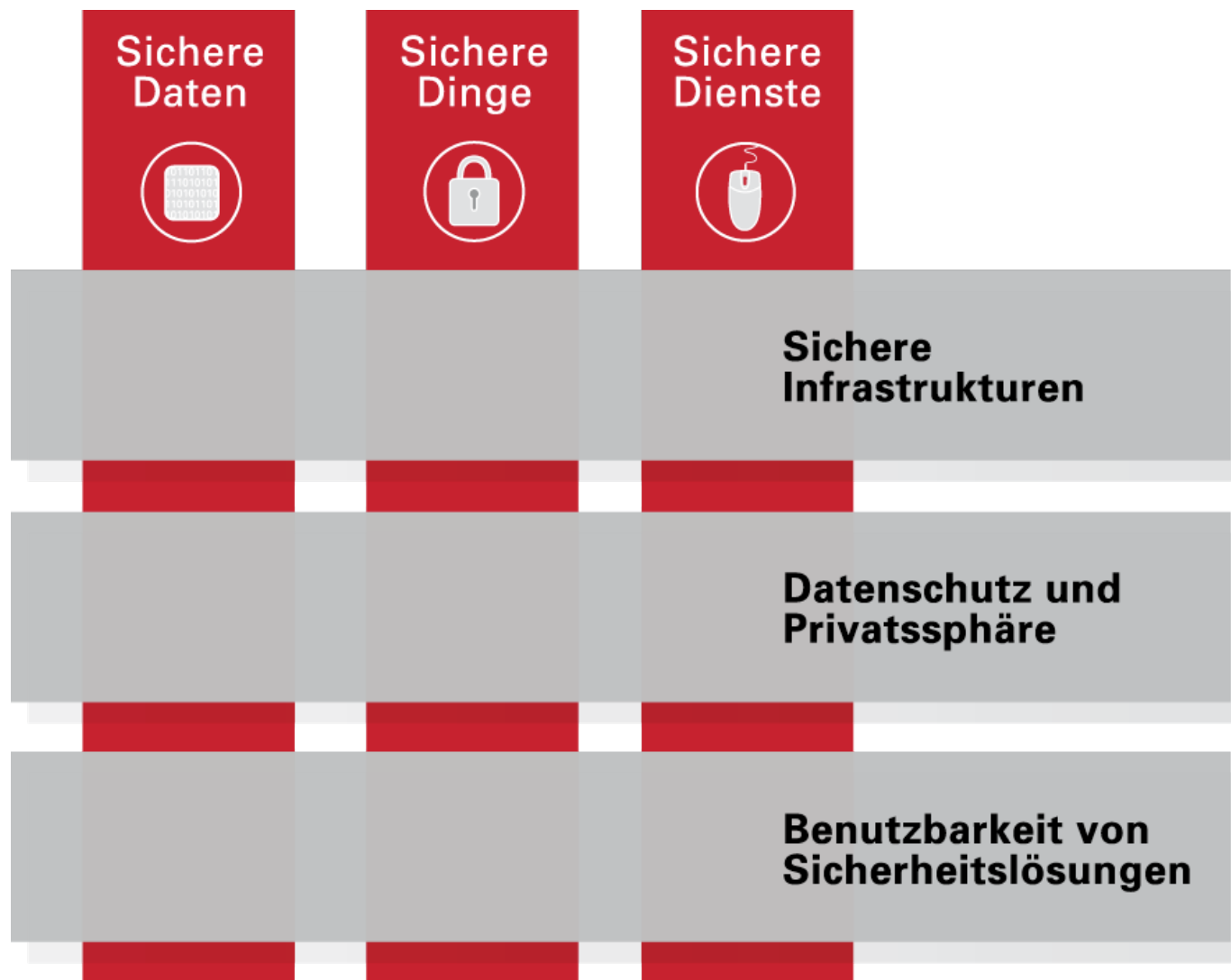
Beispiel: Physically Unclonable Function



Anfrage
„Wer bist Du?“

Originalkarte von
Erika Mustermann

Querschnittsbereiche



Forschungsgruppe da/sec der h_da



■ Biometrics and Internet-Security



Zugangskontrolle - Authentisierung

Biometrie

Mobile Systeme

Digital Forensik

Malware Detection

Intrusion Prevention

<http://www.dasec.h-da.de/>

Dr. Claudia Nickel - **the way you walk**

Motivation

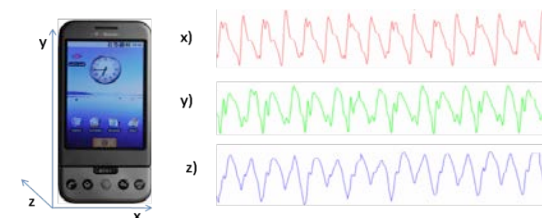
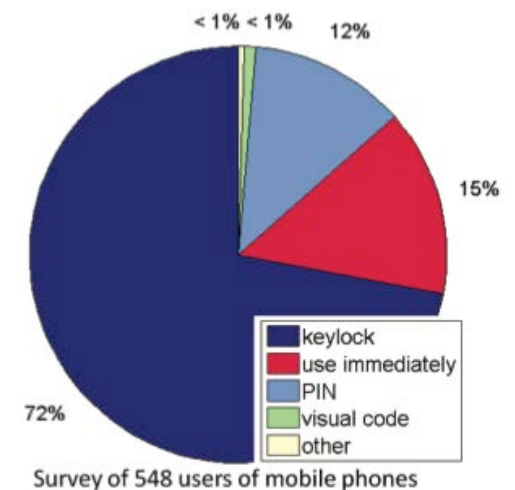
- Daten in mobilen Geräten sind üblicherweise nicht ausreichend geschützt
- Normal-Fall: Keine PIN nach Ruhezustand

Ziel

- Nebenläufige biometrische Authentisierung ersetzt PIN

Ansatz

- Erfassung der Gang-Charakteristik durch integrierten Beschleunigungssensor



Martin Olsen - **predicting Biometric Performance**



Motivation

- Grenzkontrolle im VIS erfordert gute Fingerbilder
- Fingerbildqualität bedingt gute Erkennungsleistung

Ziel

- Neue Implementierung NFIQ2
- Leichte Implementierung für mobile Systeme

Ansatz

- Erforschung von Merkmalen, die Bildqualität und Erkennungsleistung korrelieren



Intrusion Prevention System



Mark Seeger - **off-host host-observation**



Motivation

- Host basierte intrusion detection system (IDS) bedingen eine intrinsische Abhängigkeit von der Sicherheit des Host-BS
- Angreifer können ein IDS leicht manipulieren/ausschalten

Ziel

- Auslagerung der Überwachung auf die GPU und observierender Zugriff auf CPU Speicher

Ansatz

- Host-unabhängige Ausführung von GPU Kernels



Frank Breitinger – fuzzy hashing



Motivation

- Kriminelle verändern bekannte, strafbare Dateien 'leicht', damit diese nicht automatisiert erkannt werden
- Datenschutz-konforme Hinterlegung biometrischer Merkmale

Ziel

- Konstruktion einer ähnlichkeitserhaltenden Hashfunktion für Computer-Forensik u. Biometrie

Ansatz

- Context-Triggered Piecewise Hashing (CTPH)
- Evaluation eigener Ansätze

Anika Pflug – **caught in the act**



Motivation

- Bilder von Überwachungskameras sind häufig der einzige Hinweis auf die Identität von Straftätern
- 2D Gesichtserkennung wird instabil bei Posenvariationen, Gesichtsausdruck und Verdeckung

Ziel

- Multimodales Identifikationssystem basierend auf 3D Ohren und Gesichtsmerkmalen



Ansatz

- Verbindung von lokalen und holistischen Merkmalen

Sebastian Abt – **cleaning the net**



Motivation

- Cybercrime stellt ein zentrales Problem des Internets dar
- Botnetze bilden die infrastrukturelle Basis für Cybercrime

Ziel

- Effiziente und datenschutzfreundliche Detektion von Botnetz C&C-Strukturen in Netzwerken

Ansatz

- Netzwerk-Flowdaten werden mittels ML-Verfahren analysiert und korreliert, um Botnetzaktivitäten frühzeitig erkennen zu können

Best Ph.D. Thesis IT-Sicherheit - Preis 2011



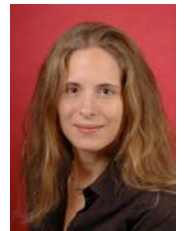
- Gesellschaft für Informatik e.V. (GI) and CAST e.V.

- Dr. Xuebing Zhou



"Privacy and Security Assessment of
Biometric Template Protection."

Masterarbeit IT-Sicherheit - 1. Preis 2011



- CAST e.V.

- Anika Pflug

"Finger Vein Recognition"

Masterarbeit IT-Sicherheit - 2. Preis 2011



- Sebastian Abt

"Assessing Semantic Conformance of
Minutiae-based Feature Extractors"

**Vertiefungsrichtung IT-Sicherheit im Masterstudiengang
der Hochschule Darmstadt**

**Masterstudiengang IT Security an der TU Darmstadt inkl.
CASED-Hacker-Contest**

**Dualer Bachelorstudiengang IT-Sicherheit an der
Hochschule Darmstadt**



▪ **Vertiefung im Master Informatik**

- Nachweis von einschlägigen 30 ECTS
- Masterarbeit zur IT-Sicherheit
- Ziel: 12 Absolventen pro Jahr ab 2013
- Ausbau Lehrangebot:

▪ **Vorlesungen:**

- 20 ECTS vor CASED --> 55 ECTS durch CASED 1
- Dezidierte Seminare u. Projekt Systementwicklung IT-Sec

▪ **Zitat einer Studierenden:**

- *'Ich habe vorher Informatik an der HS Bremen studiert.
Wegen der Vertiefung IT-Sec im Master Informatik
bin ich an die h_da gewechselt.'*

Lehrkooperation

■ Lehrkooperation mit der TUD:

- Seit SS 2010
- Komplementäre LV werden für die Partner-Hochschule geöffnet
- h_da-Studierende an TUD: Hacker Contest, Netzsicherheit
- TUD-Studierende an h_da: Biometrische Systeme, Computerforensik

■ Internationalisierung des Studiums:

- Export der LV Biometrische Systeme an die DTU Kopenhagen
- Ingoing- / Outgoing-Studierende für Abschlussarbeiten (FH OÖ, DTU, KTH, NISlab)

■ Fachgruppe IT-Sicherheit

- Zur Zeit sind Professoren aus 3 Fachbereichen beteiligt



Mitglieder der Fachgruppe

- Sebastian Abt (FbI, CASED)
- Prof. Dr. Harald Baier (FbI, CASED)
- Prof. Dr. Michael Braun (FbI)
- Prof. Dr. Christoph Busch (Media, CASED)
- Prof. Dr. Woldemar Fuhrmann (FbI)
- Prof. Dr. Klaus Kasper (FbI)
- Prof. Dr. Bernhard Kreling (FbI)
- Prof. Dr. Steffen Lange (FbI)
- Christian Maaser (FbI, CASED)
- Jutta Müller (FbI)
- Prof. Dr. Michael Massoth (FbI)
- Claudia Nickel (FbI, CASED)
- Prof. Dr. Reiner Nitsch (FbI)
- Mark Seeger (FbI, CASED)
- Wolfgang Ottenbacher (FbI)
- Prof. Dr. Alois Schütte (FbI)
- Jens Weibler (FbI)
- Prof. Dr. Thomas Wilmer (GS)
- Prof. Dr. Peter Wollenweber (FbI)

- <http://www.fbi.h-da.de/organisation/fachgruppen/fachgruppe-it-sicherheit.html>

Technische Verantwortung: Zugangskontrolle

Authentisierungs Faktoren

Zugangskontrolle

Eine Authentisierung kann erreicht werden:

- durch **Wissen**:
Password, PIN, ...

Zugangskontrolle

Statistik basierend auf 32 Millionen Passwörtern

- 20% sind Namen und triviale Passwörter
- Top 5 passwords (@ www.rockyou.com)

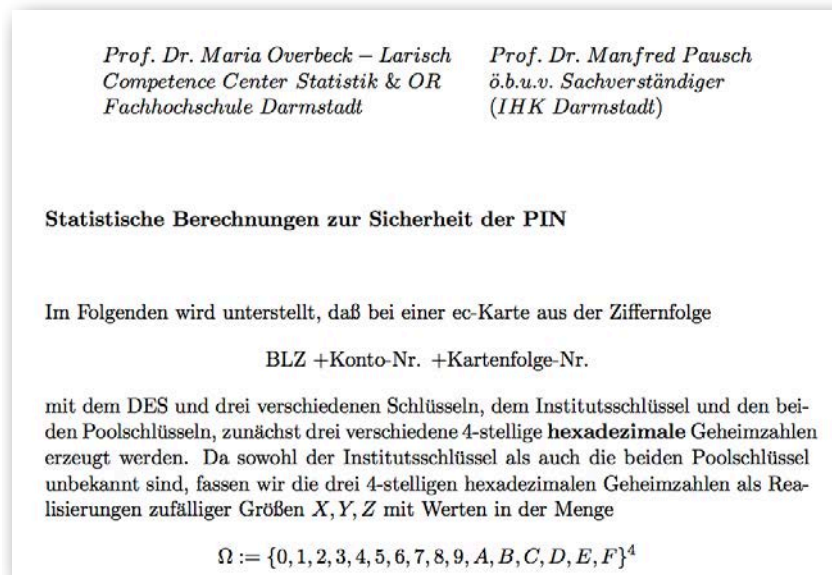
Rank	Password	Number of Users with Password (absolute)
1	123456	290731
2	12345	79078
3	123456789	76790
4	Password	61958
5	iloveyou	51622

Source: Imperva

Zugangskontrolle

Sicherheit von PIN - im Jahr 1998

- „*Statistische Berechnungen zur Sicherheit der PIN*“
Maria Overbeck-Larisch (FHD, Darmstadt) und
Manfred Pausch (Sachverständiger, IHK Darmstadt)



„Hat der Karteninhaber tatsächlich eine dieser Geheimzahlen, so hat er mit einer Wahrscheinlichkeit von $\approx 11\%$ davon auszugehen, daß bei Verlust der Karte sein Konto geplündert wird.“

- Merke: wenn Ihre Debit-Karte die **PIN 1020** hat, dann
 - tauschen Sie Ihre Karte bei der Bank ein oder
 - fragen Sie Frau Overbeck-Larisch um Rat

Zugangskontrolle

Eine Authentisierung kann erreicht werden:

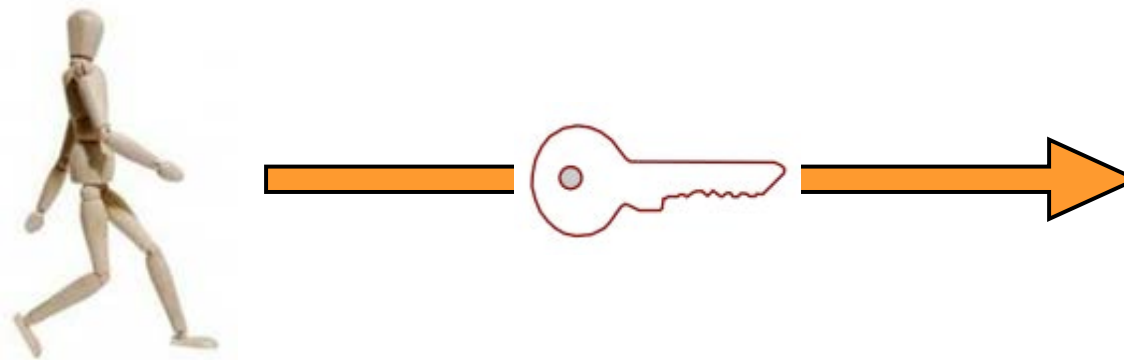
- durch **Wissen**:
Password, PIN, ...
- durch **Besitz**:
SmartCard, USB-token, key



Zugangskontrolle

Traditionell etablieren wir zwischen

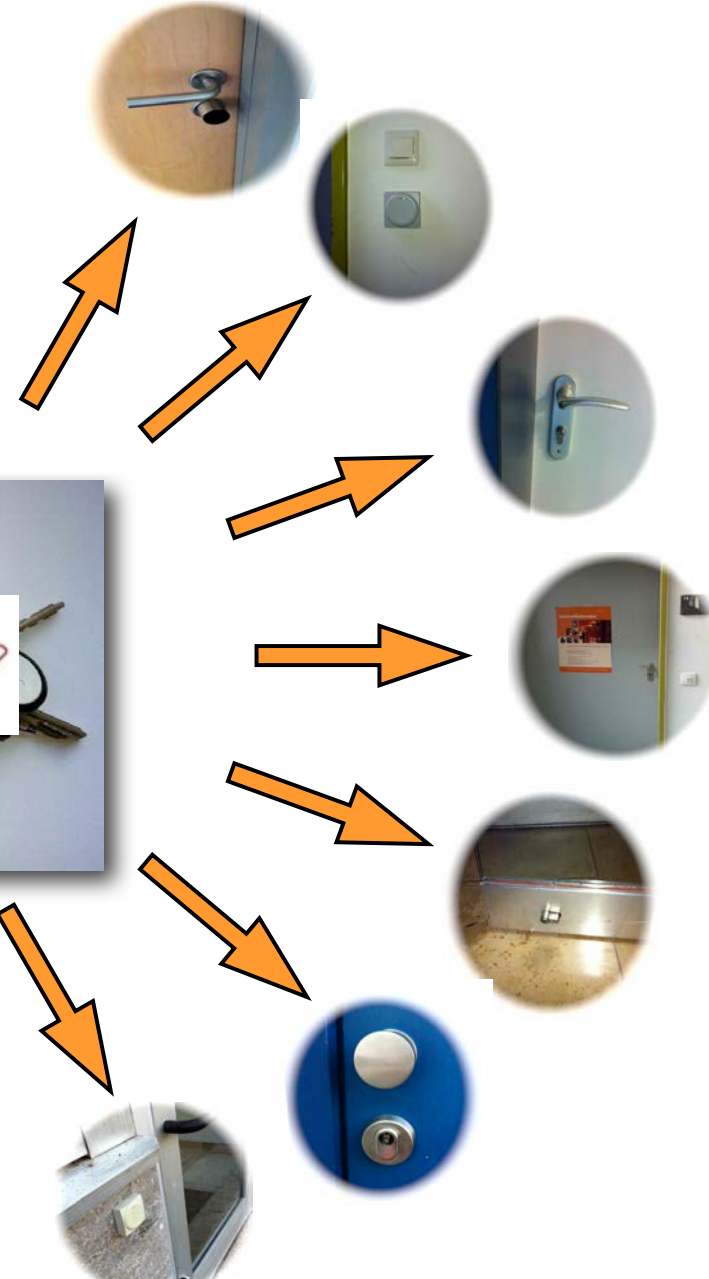
- natürlichen Personen
- und Objekten
- einen Token (d.h. einen Schlüssel)



Zugangskontrolle

Aber in der **Realität** haben wir

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



Zugangskontrolle

In der Zukunft werden wir Karten haben

- die uns Zugang gewähren
- aber zu **vielen** Türen



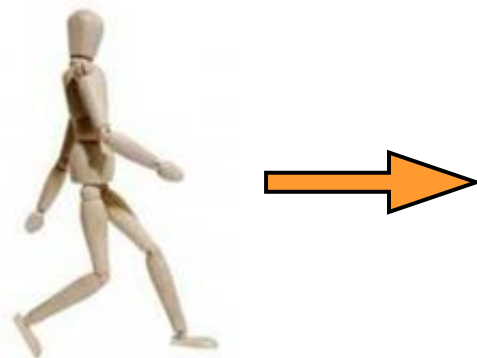
Campus Card



Zugangskontrolle

Für einige Personen

- ist die Sammlung der Karten schon heute **eindrucksvoll** und **unhandlich**



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.

- Sicherheitspolitik kann nicht durch Delegation umgangen werden!
- Eine Transaktion kann nicht abgestritten werden
 - „das muss *Igor Popov* mit meiner Karte gewesen sein ...“

Wie funktionieren biometrische Systeme?

Beispiel: Fingerabdruck-Erkennung

Analoge/digital Repräsentation der Papillarleisten

- Landmarken im Fingerbild: **Minutien**

Bifurcations

Ridge endings

Singularity



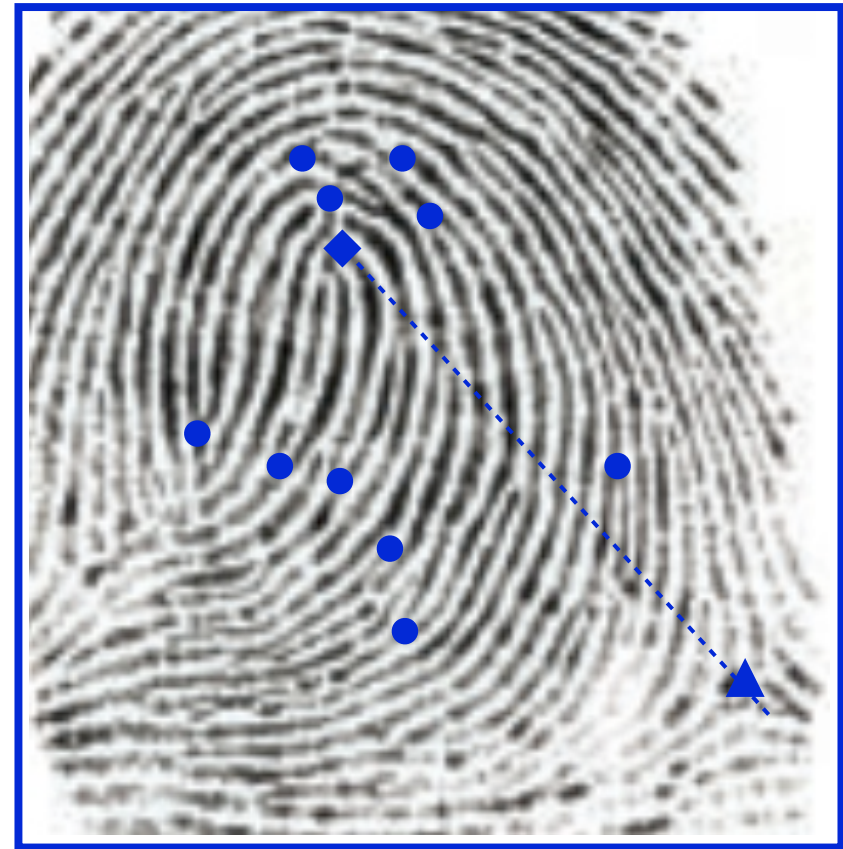
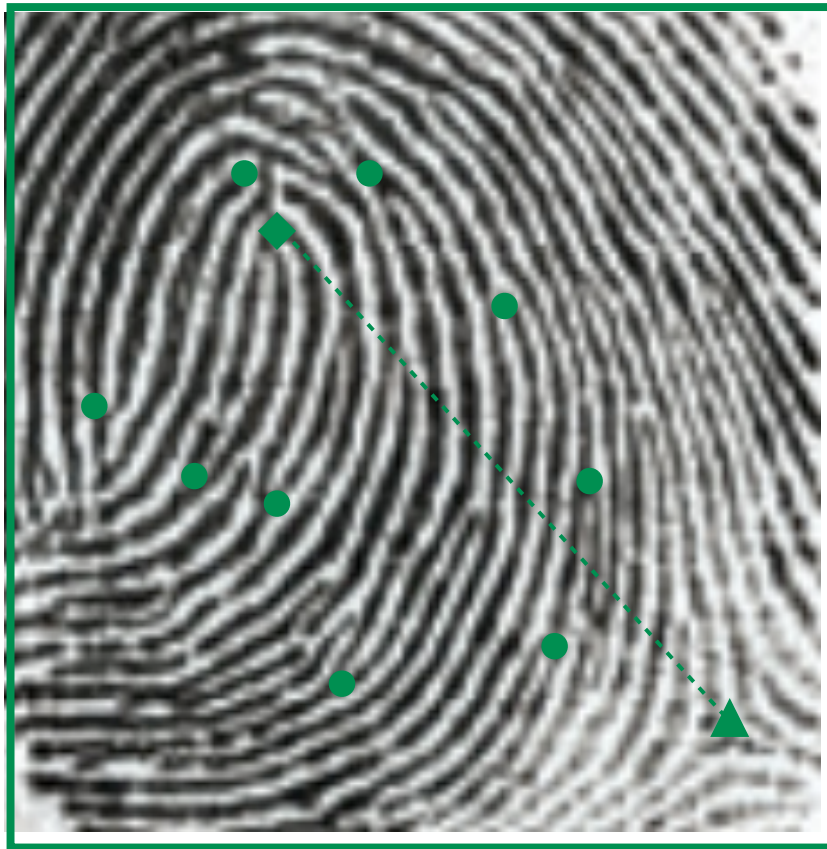
Beispiel: Fingerabdruck-Erkennung

Vergleich des **Reference** Image
mit dem **Probe** Image



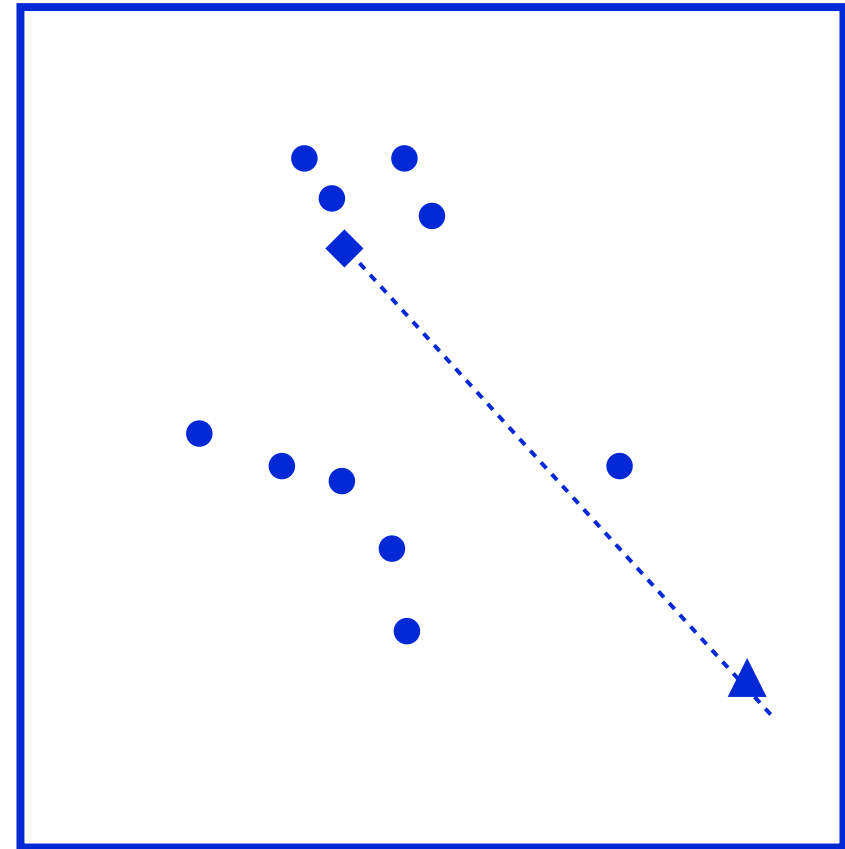
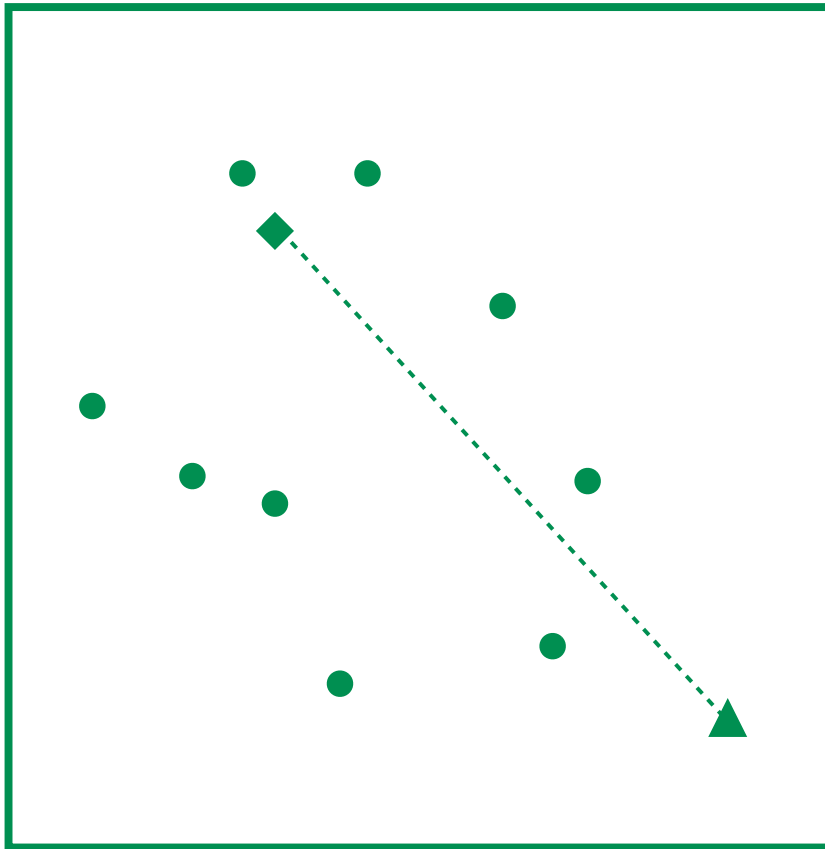
Beispiel: Fingerabdruck-Erkennung

Vergleich des **Reference** Image
mit dem **Probe** Image



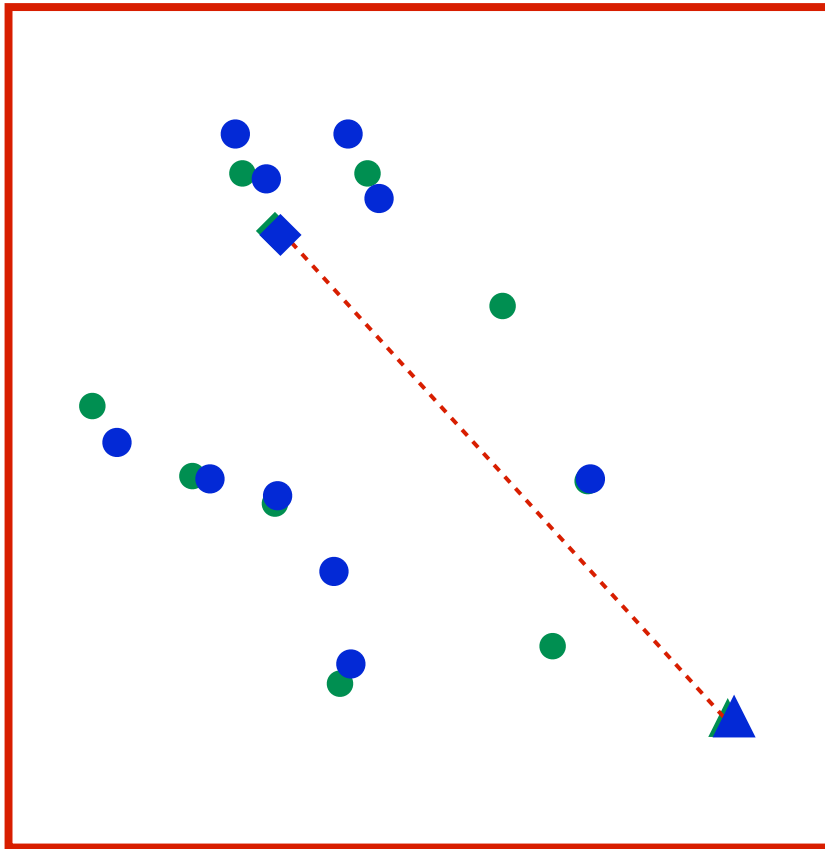
Beispiel: Fingerabdruck-Erkennung

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**“)

Identifikation - Verifikation

Identifikation:

- Erkenne die Identität einer Person (1:n - Vergleich)



staff identity = „busch“

Verifikation:

- Validierung einer Identitätsbehauptung (1:1 - Vergleich)



similarity: „71%“
(Comparison-Score)

Biometrische Charakteristika

Wichtige Eigenschaften

- **Allgemeingültigkeit** – jeder sollte dieses Charakteristikum aufweisen
- **Einzigartigkeit** – wie gut lassen sich Individuen unterscheiden?
- **Dauerhaftigkeit** – wie stark verändert es sich mit der Zeit?
- **Erfassbarkeit** – ist eine einfache Messung möglich?
- **Akzeptanz** – Grad der Zustimmung durch Nutzer
- **Umgehung** – lässt sich ein Artefakt (Gummifinger) nachbilden?
- **Performanz** – Erkennungsleistung und Geschwindigkeit

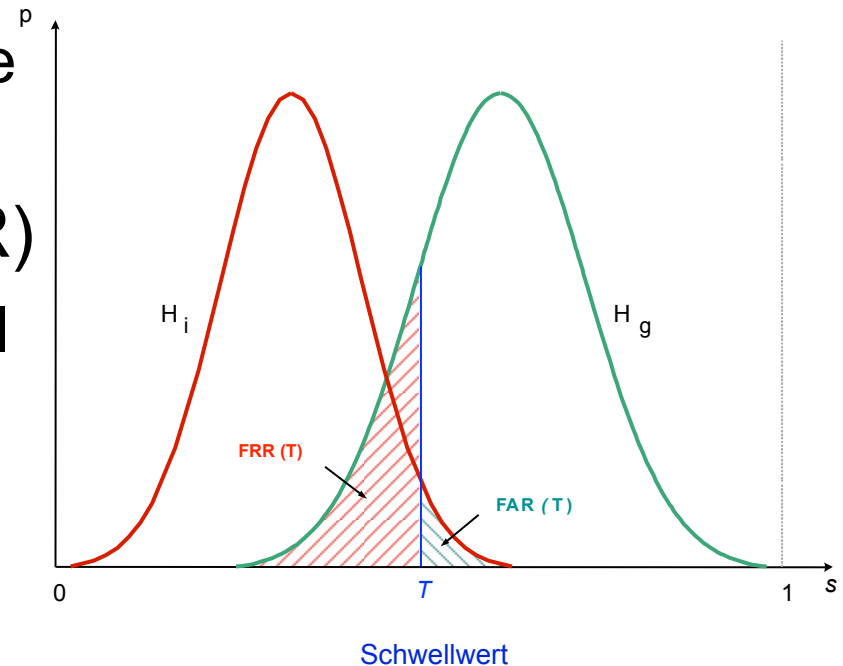
Erkennungsleistung

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



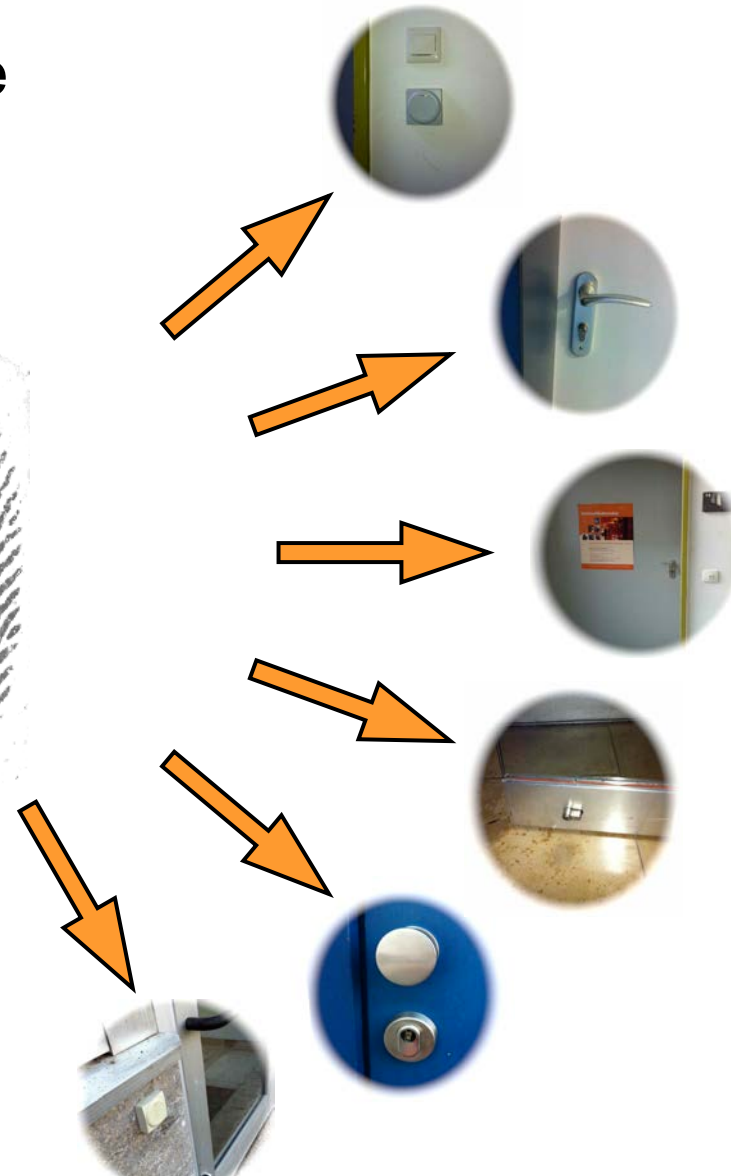
Biometrie in der Zugangskontrolle

Sollte es

- **biometrische** Zugangskontrolle an jeder Tür geben?



- **Kosten-Faktor** Sensoren?
- Wo **Referenzen** hinterlegen?



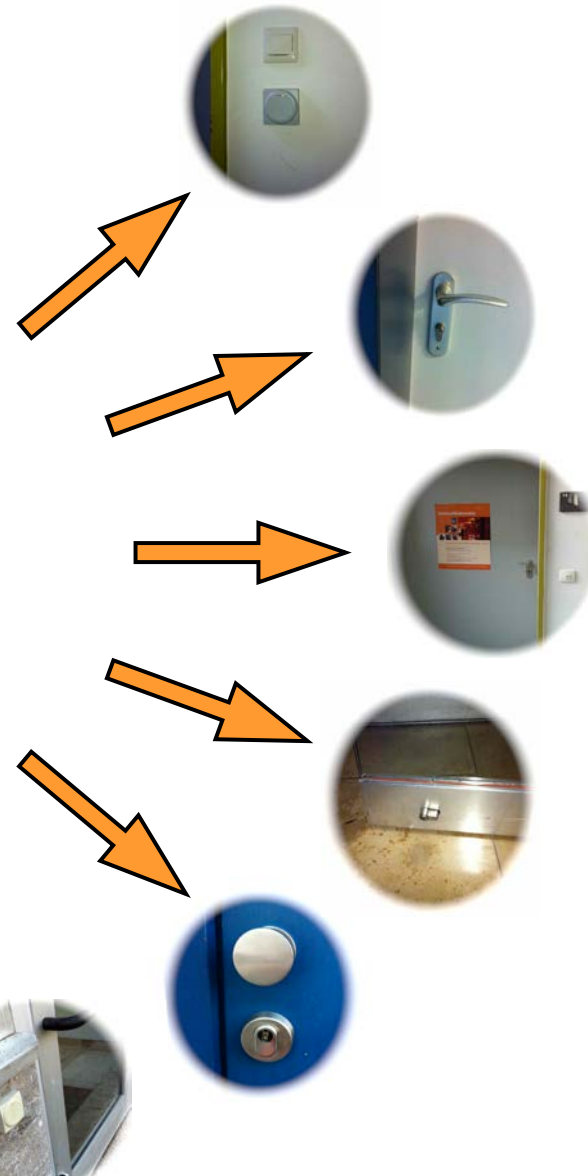
Smartphone Based Access Control

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)

Near Field Communication (NFC)

Weit verbreitete Technik in Smartphones

- Short range wireless communication im Bereich 13,56 MHz
 - basiert auf **passive** RFID technology (ISO 14443)
 - oder **aktiver** Kommunikation
- Arbeitsbereich **proximity** Distanz bis 20 cm



Smartphone - der Persönliche Assistent

Smartphones sind schon heute das **dominante** persönliche Endgerät

- 417 mobile phones sold to end users in the 3rd quarter of 2010 (Gartner, 2010)
- 96% growth of Smartphone sales from 2009 to 2010. Smartphone accounted for 19,3% percent of overall mobile phone sales in the thirrd quarter of 2010. (Gartner, 2010)
- „*By 2013 Phones will overtake PCs as dominant web access device*“ (Gartner, 2010)

Und wer sichert den Zugang zum Smartphone?

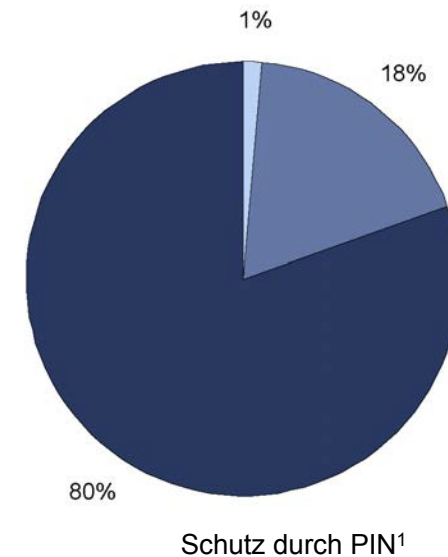
Bedrohungssanalyse

Daten in **mobile Geräten** sind in der Regel **ungeschützt**
keine PIN-Authentisierung nach Ruhe-Zustand

- Umfrage-Ergebnis:
nur 18% nutzen PIN code

Alle **Daten** auf dem Smartphone
sind **frei** zugänglich

- Emails, Adressen,
- Termine, Photos
- PINs etc.



Grund:

- PIN-Authentication ist aufwändig und umständlich

¹F. Breitingner, C. Nickel: User Survey on Phone Security, BIOSIG 2010

Smartphone - Zugangskontrolle

Foreground authentication (Nutzer **Interaktion**)

- **Kamera**-Sensor
 - **Fingerabdruck**erkennung
 - Gesichtserkennung
 - Iriserkennung



Background authentication (**Beobachtung** des Nutzers)

- Microphone
 - **Sprecher**erkennung
- Accelerometer - Beschleunigungssensor
 - **Gang**erkennung
 - nebenläufig ohne Beeinträchtigung

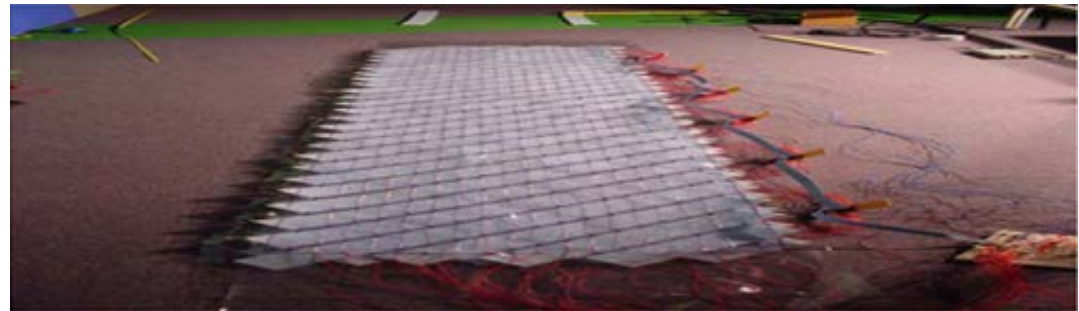
Gangerkennung

Biometrische Gangerkennung

- Machine Vision



- Floor Sensors



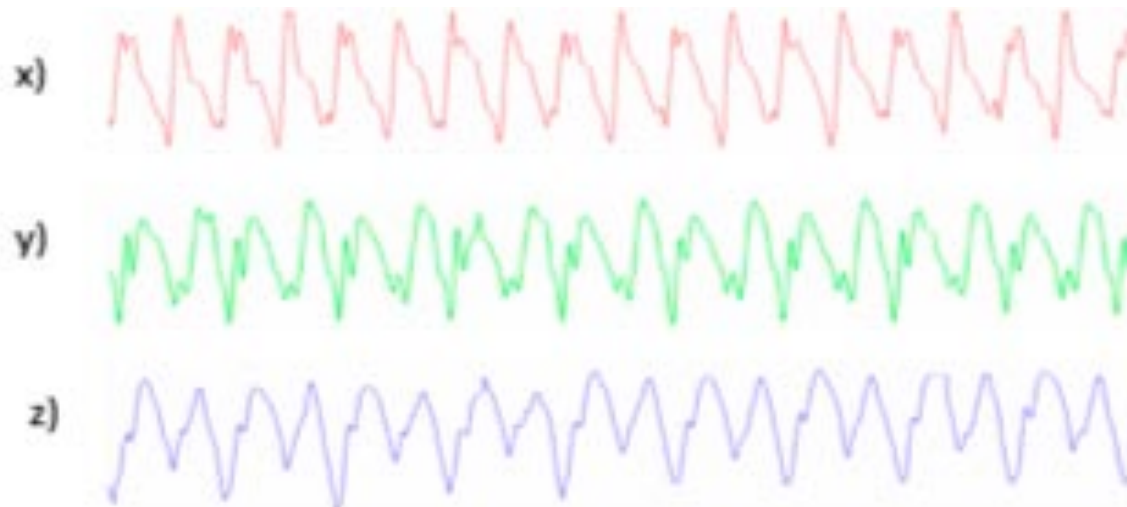
- Wearable Sensors



Biometrische Gangerkennung

Erlaubt eine **nebenläufige** Authentisierung durch Analyse des Schrittmusters

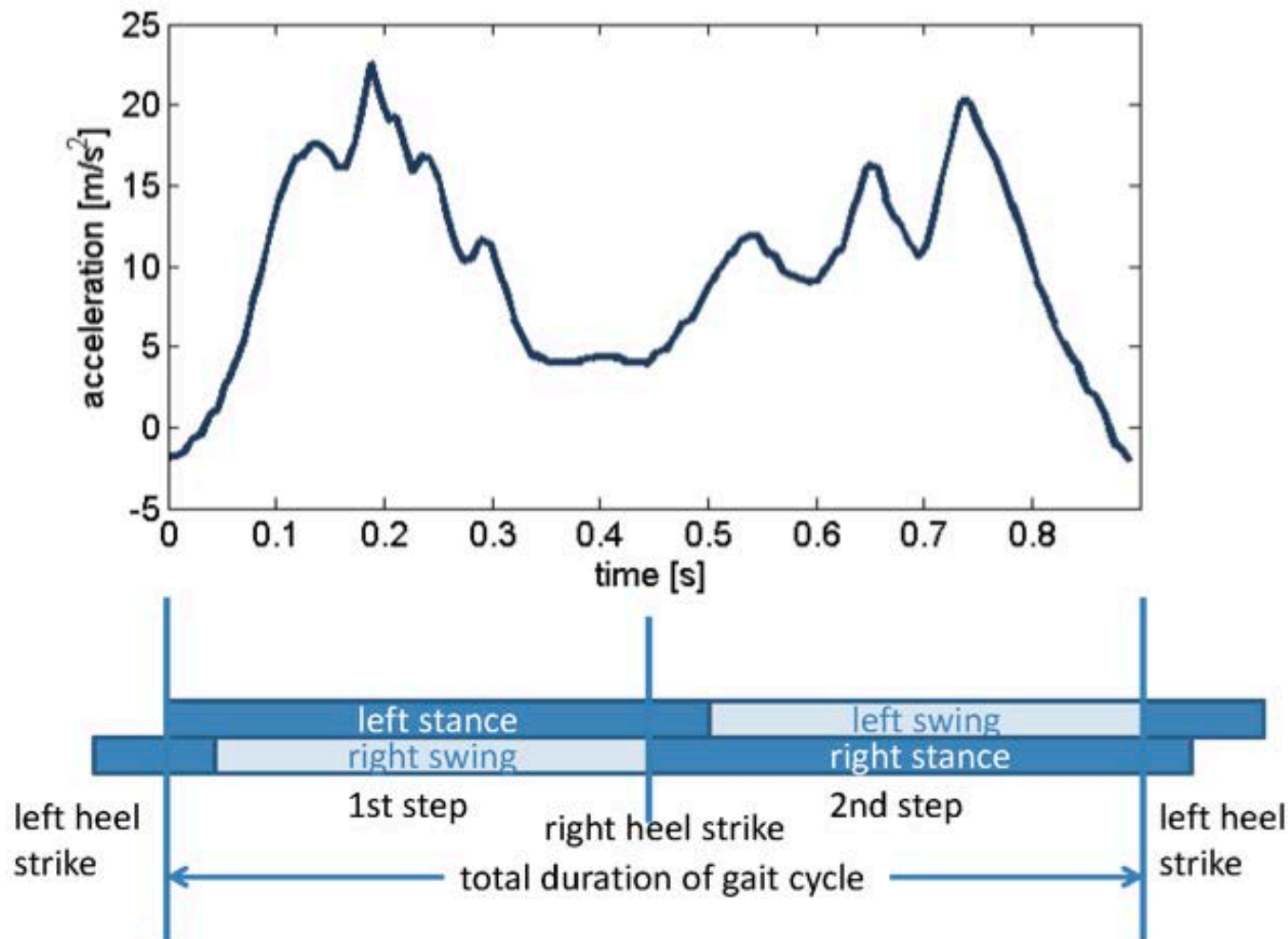
- Nutzung von **Beschleunigungs-Sensor** - die ohnehin im Mobilgerät verbaut sind
 - Die meisten Smartphones enthalten einen **Accelerometer**
 - Biometrie ohne Sensor-Kosten
 - Beschleunigung in drei Richtungen



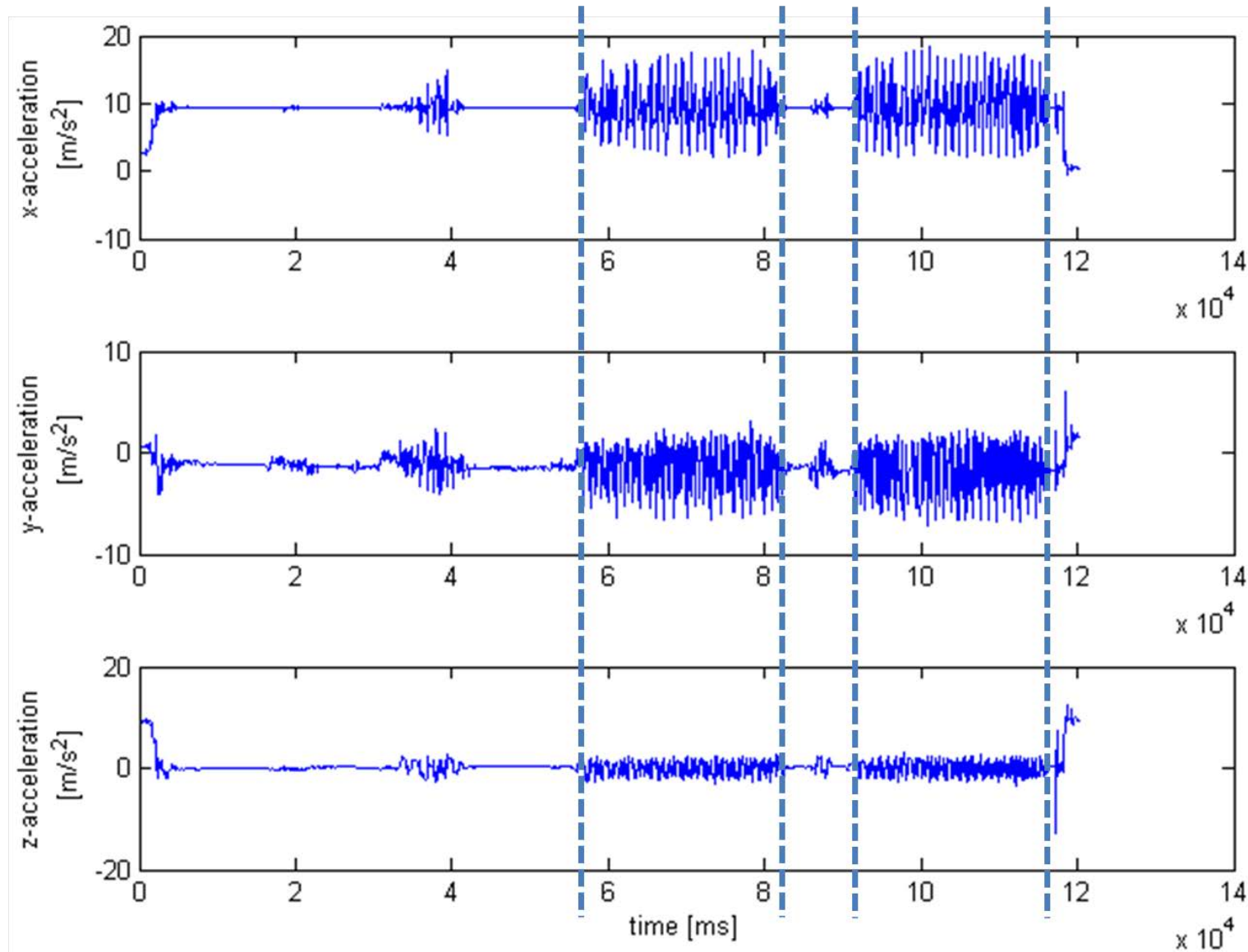
Biometrische Gangerkennung

Aufzeichnung des Schrittmusters

- Periodisches Muster



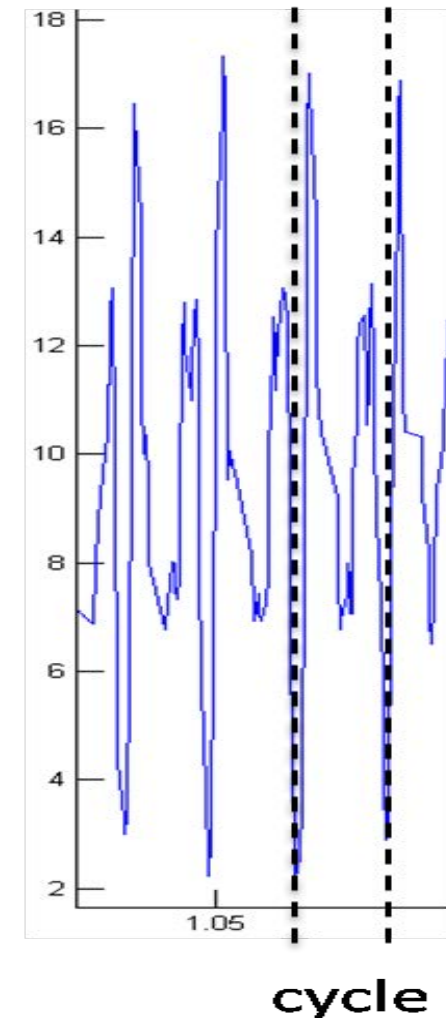
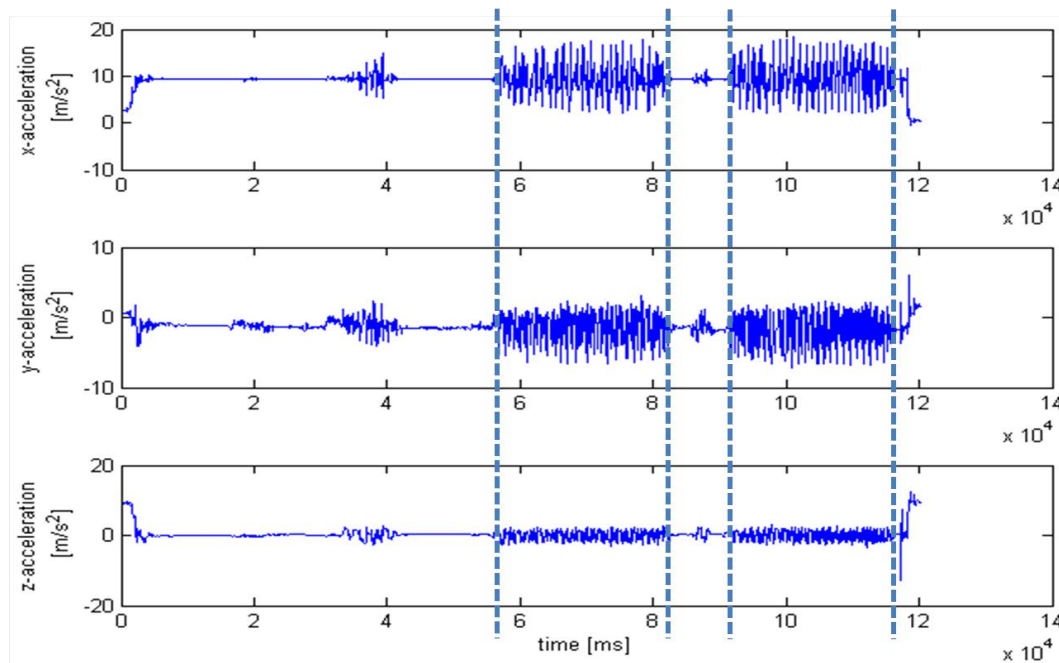
Daten Beispiel



Gangerkennung - Enrolment

Processing

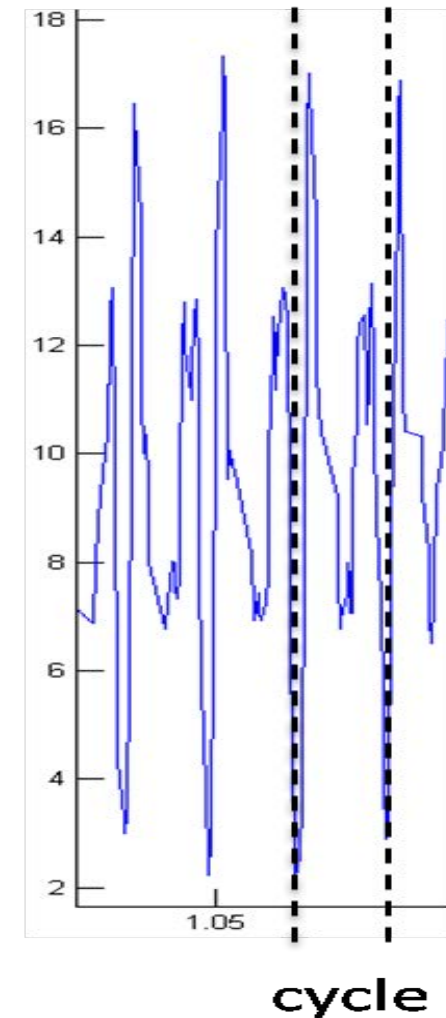
- Reference-Cycle wird aus dem Signal **segmentiert**



Gangerkennung - Enrolment

Signalverarbeitung

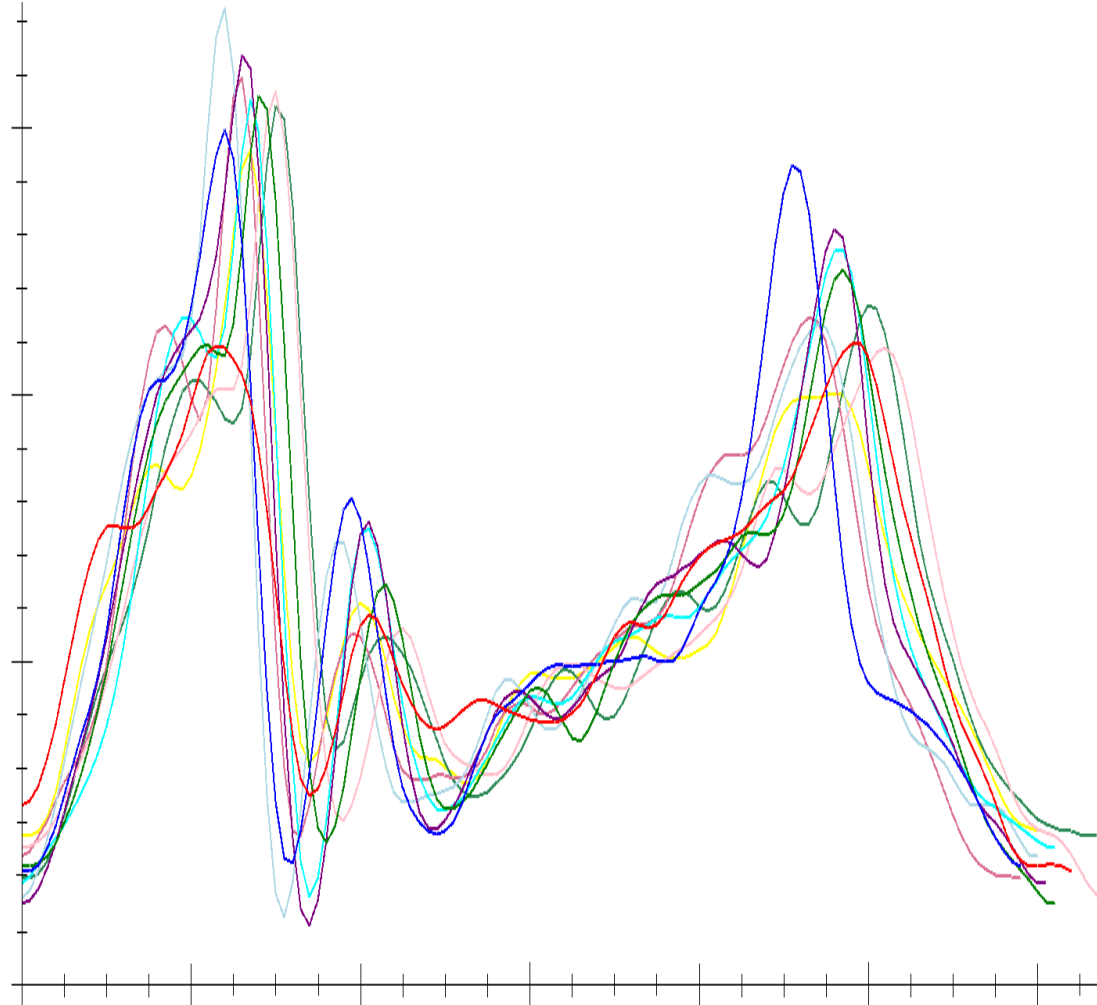
- Merkmalsextraktion:
kompakte **Beschreibung** eines Zyklus
 - Mean, maximum, minimum, standard deviation
 - Binned distribution (5 bins)
 - Root mean square
 - Zero crossings
 - Mel-Frequency Cepstral Coefficients
 - Bark-Frequency Cepstral Coefficients
- Die berechneten Merkmale werden als biometrische **Referenz** im Smartphone gespeichert



Gangerkennung - Zuverlässigkeit?

Niedrige **Intra**-Class Varianz

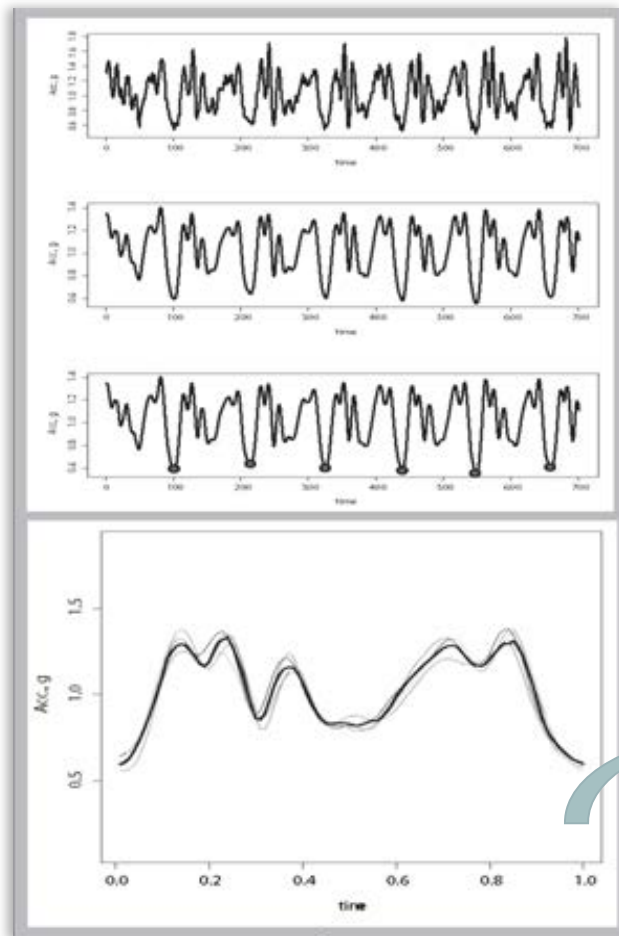
- Hohe inter-class Varianz



Gangerkennung - Verifikation

Enrolment

Imposter **Verifikations** Versuch



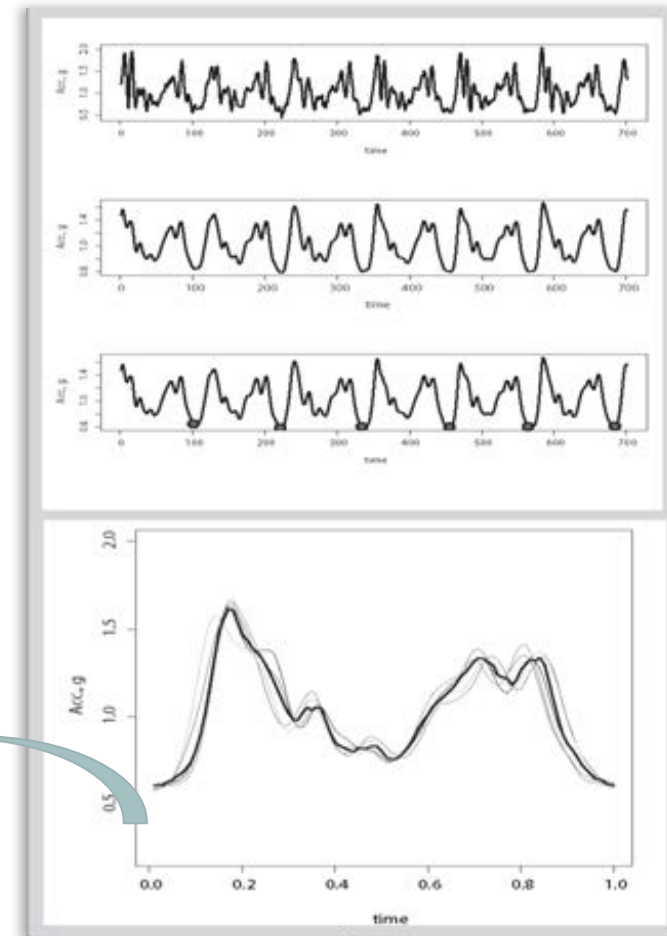
Raw Cycle

Noise reduction

Cycle Detection

Average Cycle

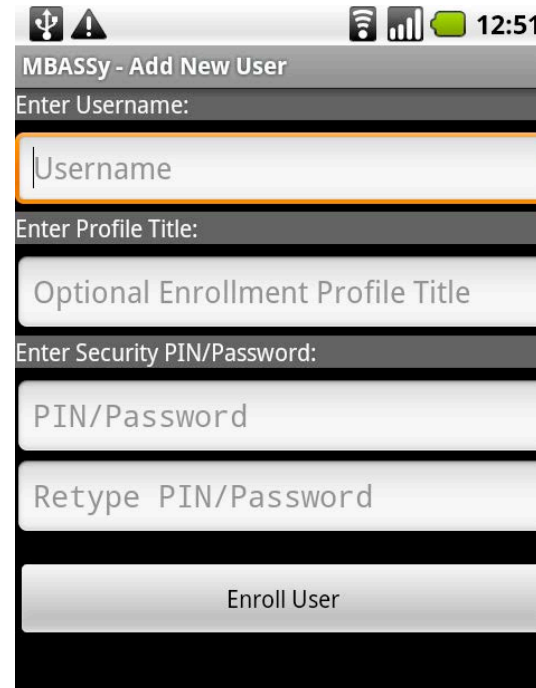
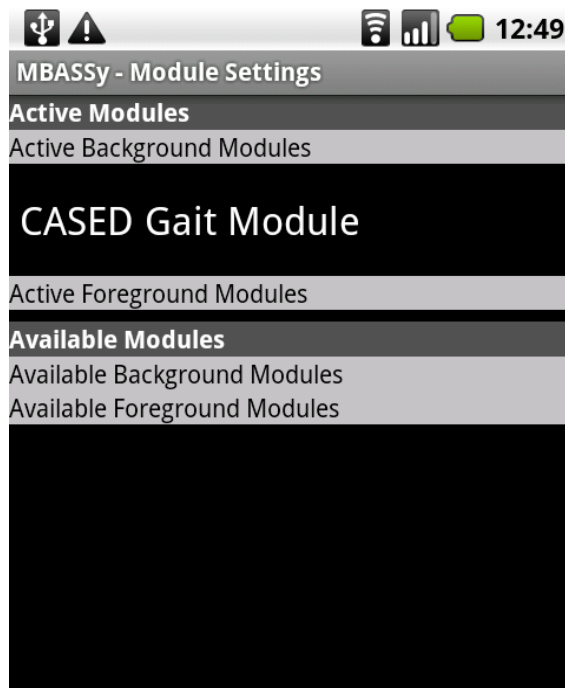
Comparison Score



Authentisierung an Smartphones

Modular Biometric Authentication Service System

- System für Android
- Verschiedene Module können integriert werden
 - Gang, voice, fingerprint, Graphische Authentisierung, ...

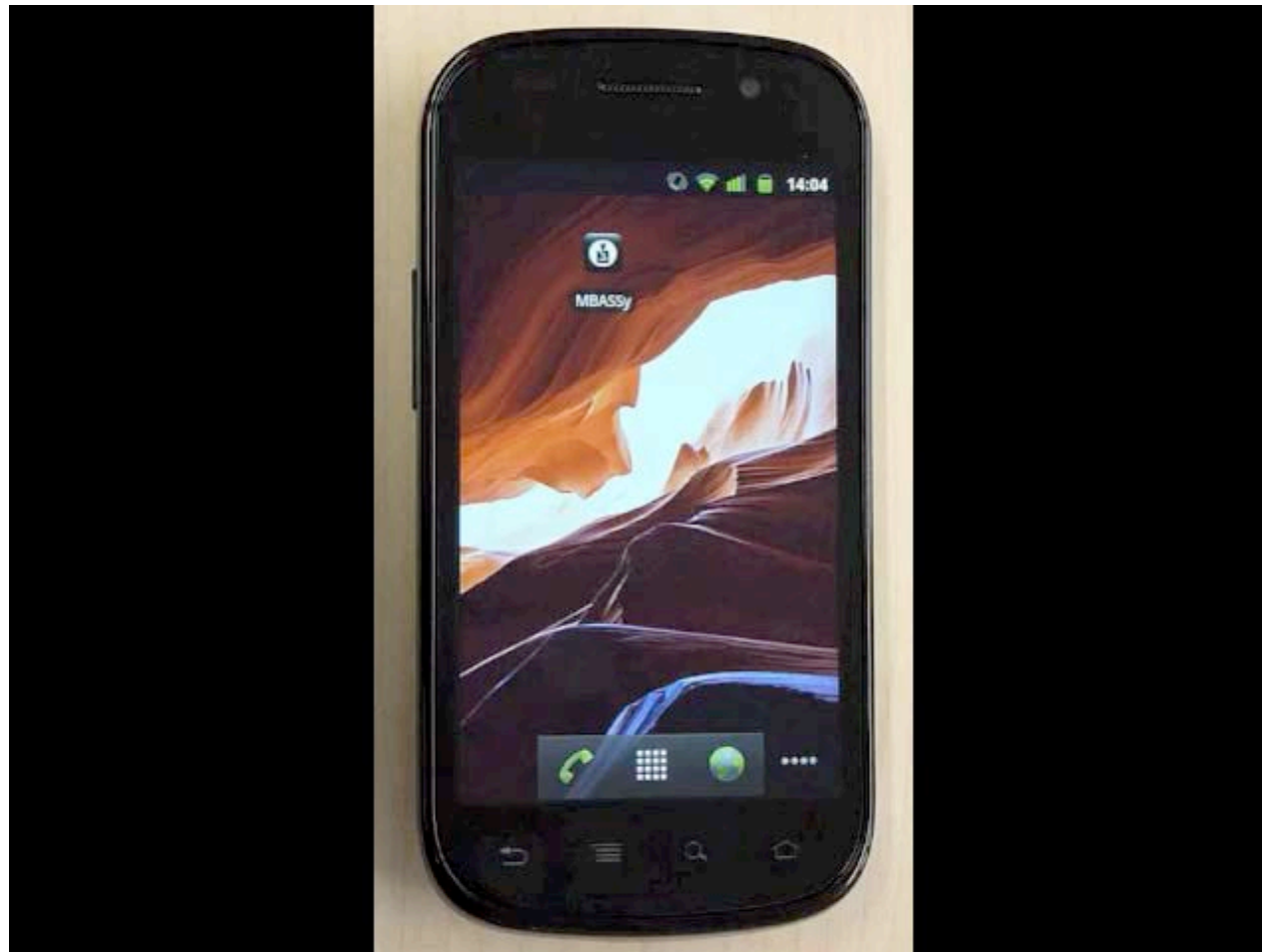


<http://www.dasec.h-da.de/research/biometrics/mbassy/>

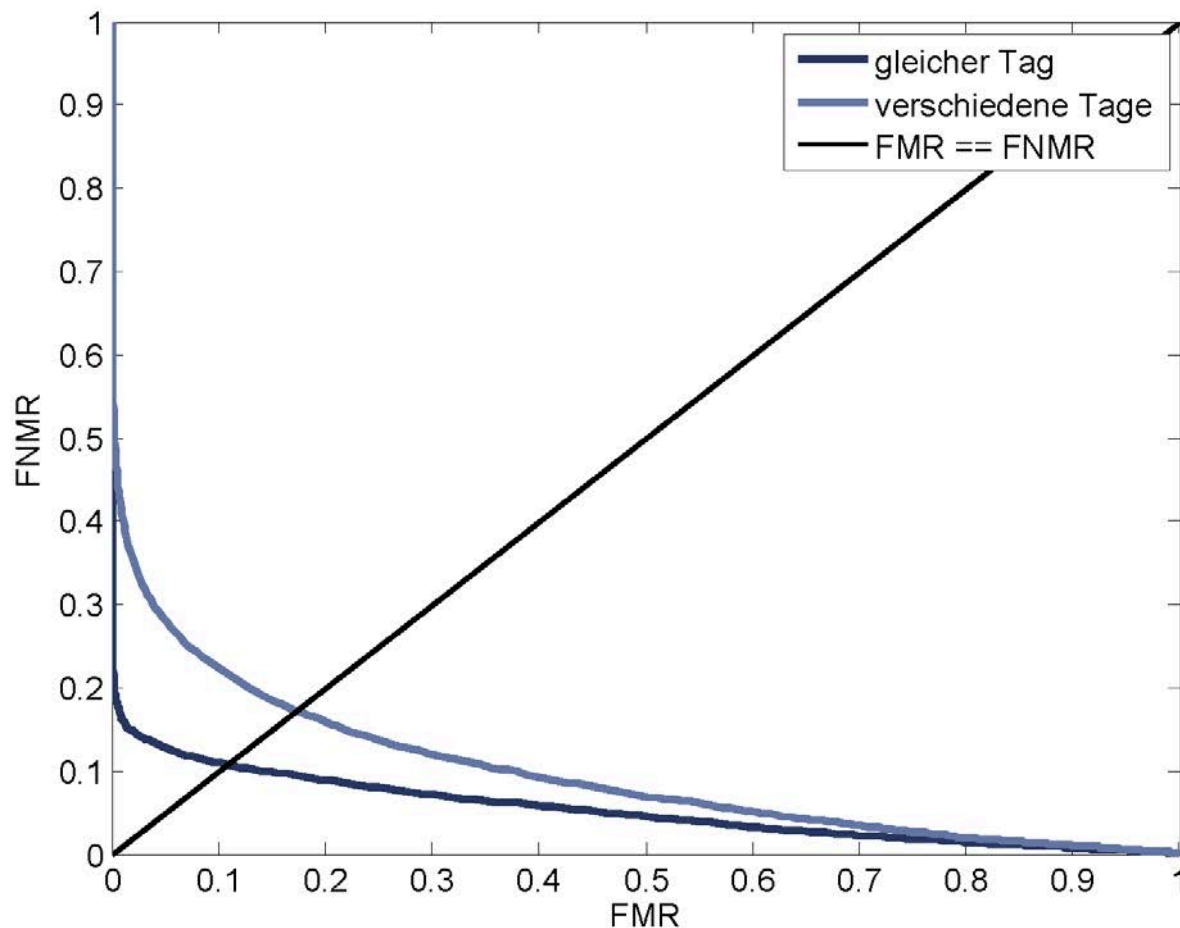
Authentisierung an Smartphones

Modular Biometric Authentication Service System

- MBASSy - Film



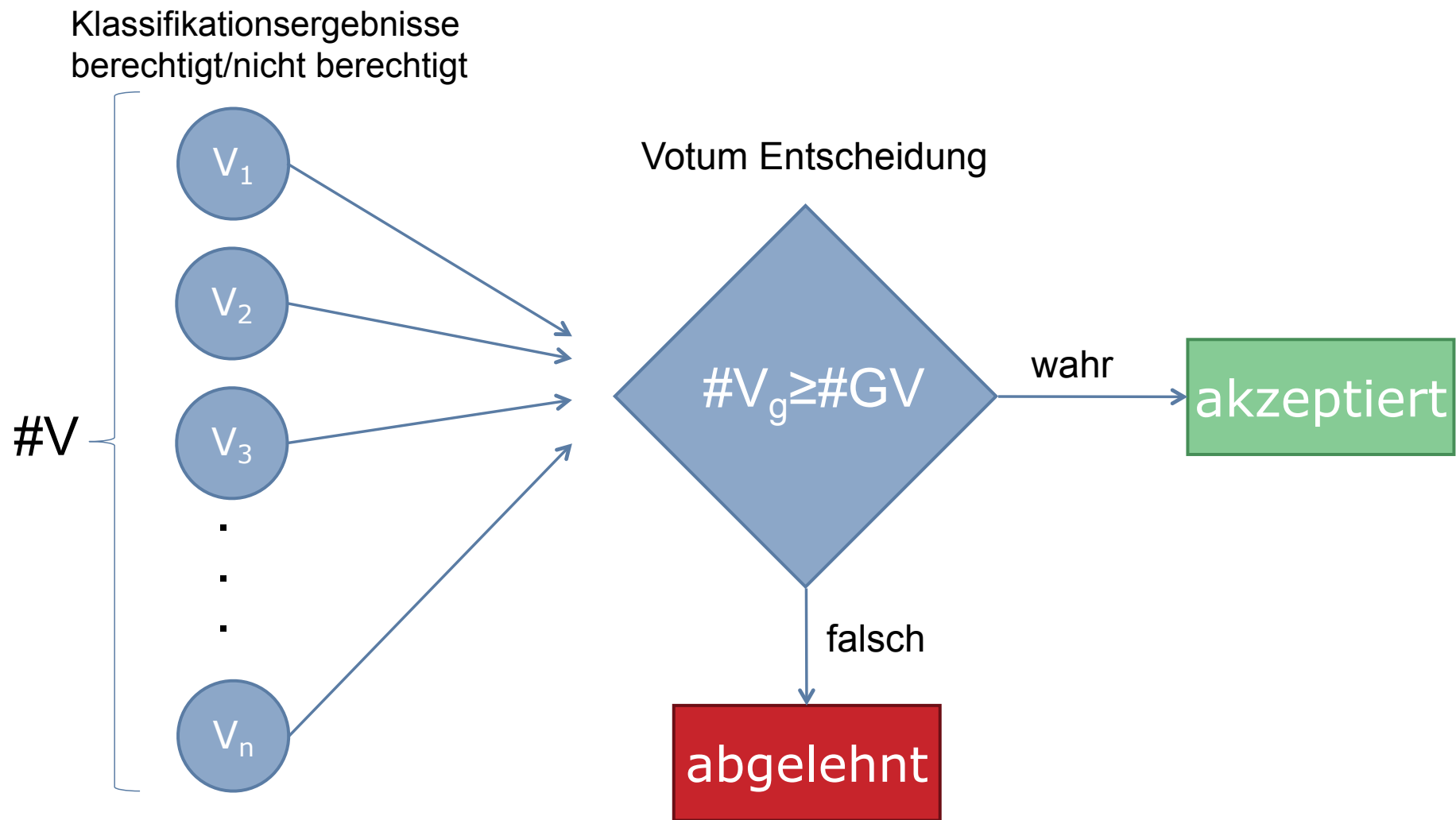
Template Alterung



Klassifikator: HMM

¹C. Nickel, C. Busch: Classifying Accelerometer Data via Hidden Markov Models to Authenticate People by the Way they Walk", 45th IEEE ICCST, 2011

Votum-Verfahren



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)

Zusammenfassung

- Biometrie kann zur Steigerung der Sicherheit eingesetzt werden
- Smartphones werden Schlüssel ablösen
- Biometrische Authentisierung am Smartphone
 - komfortabel
 - ohne neue Sensoren und damit ohne Kosten möglich
- Gangerkennung zeigt eine gute Erkennungsleistung

Kontakt



Prof. Dr. Christoph Busch
Principal Investigator

CASED
Mornewegstr. 32
64293 Darmstadt/Germany
christoph.busch@cased.de

Telefon +49 6151/16 9444
Fax
www.cased.de

Kontakt

