Biometrische Systeme und Methoden - Maschinen identifizieren Menschen!

Christoph Busch
Hochschule Darmstadt - CASED
http://www.christoph-busch.de/

Strategiegipfel: IT & Information Security

Berlin - November 17 2015
Biometric activities

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

Recent projects related to Biometrics

- Hochschule Darmstadt:
  - LOEWE CASED [http://www.cased.de](http://www.cased.de)
  - LOEWE BioMobile
- NISlab:
  - EU-FP7 FIDELITY [http://www.fidelity-project.eu](http://www.fidelity-project.eu)
  - EU-FP7 INGRESS [http://www.ingress-project.eu](http://www.ingress-project.eu)
  - EU-FP7 PIDaaS [http://www.pidaas.eu](http://www.pidaas.eu)
Introduction to Biometrics
Biometrics - Fingerprint Recognition

Analog/digital representation of the finger ridges

- Distinguished points of the fingerprint: Minutia

- Bifurcations
- Ridge endings
- Singularity
Feature Extraction and Comparison

Comparison of reference image against a probe image
Feature Extraction and Comparison

Comparison of reference image against a probe image
Feature Extraction and Comparison

Comparison of reference feature vector against a probe feature vector
Feature Extraction and Comparison

Comparison of *reference* feature vector against a *probe* feature vector
Biometric Rumors
Operators may think:

„Biometrics are not as secure as PINs“
There are striking arguments why biometric authentication is better than the PIN

• The entropy of a 4 or 6-digit PIN is very limited
  - Even for a 6 digit numeric PIN (e.g. with the German eID card) the entropy $H = L \times \log_2 N$
    is limited to less than 20bit (with $L=6, N=10$)
  - The reported entropy for different biometric characteristics is
    - Fingerprints 84bit [Ratha2001], Iris 249bit [Daugman2006]
    Face 56bit [Adler2006], Voice 127bit [Nautsch2015]

There are striking arguments why biometric authentication is better than the PIN

- PINs can be delegated in violation of the security policy
  - "This transaction was done by Mr. Popov, who was mis-using my card"
  - biometric authentication enables non-repudiation of transactions

Biometrics are better than PINs!
Operators may think:

„Biometric systems are not compliant to data privacy principles“
Biometric Template Protection

We do NOT store fingerprint, iris or face images

• we transform templates to pseudonymous identifiers (PI)
• we reach
  - Secrecy: biometric references (PI) can be compared without decryption.
  - Diversifiability / Unlinkability: Unique pseudonymous identifier can be created for each application to prevent database cross-comparison
  - Renewability: we can revoke and renew template data.
  - Non-invertibility: Original biometric sample can not be reconstructed


Protection at the same accuracy level is possible

- Bloom filter-based pseudonymous identifiers

Bloom Filter-based transformation of biometric templates

Secrecy ✓
Non-invertibility ✓
Diversification ✓
Noise robustness ✓

Biometric Template Protection enables revocability in biometric systems!
Data Protection Requirements

A technical guideline, how to implement requirements for data privacy and data protection is formulated in:

Standards?

Operators *may* think:

„*There are no standards on biometrics*“
Biometric Standardisation

International Organization for Standardisation

Joint Technical Committee One

International Electrotechnical Commission

International Civil Aviation Organization

TC 68
Banking, Securities
Financial services

SC 17
Cards & Personal Identification

SC 27
IT Security Techniques

SC 37
Biometrics

SC37 to TC68

SC 37 Formal Liaisons
ISO/IEC Interchange Format Standards

The 19794-Family: Biometric data interchange formats

All parts binary encoding
Generation 2 of ISO/IEC 19794

All parts binary encoding

the semantic is equivalent for binary encoded and XML encoded records
Operators will think:

„The biometric sensors must be robust against fake attacks“
Gummy Finger Production in 2000!

Attack \textit{without} support of an enroled individual

- Recording of an analog fingerprint from flat surface material
  - z.B. glass, CD-cover, etc.
  - with iron powder and tape

- Scanning and post processing:
  - Correction of scanning errors
  - Closing of ridge lines (as needed)
  - Image inversion

- Print on transparent slide

- Photochemical production of a platine
Gummy Finger Production in 2000!

Reported in a publication by BKA

Presentation Attack Detection

ISO/IEC 30107 - Definitions

- **presentation attack instrument (PAI)**
  biometric characteristic or object used in a presentation attack

- **artefact**
  artificial object or representation presenting a copy of biometric characteristics or synthetic biometric patterns

Types of presentation attacks

(Genral Noun)

(Adjectives describing categories)

(Qualifying adjectives)

Source: ISO/IEC 30107-1
Acceptability?

Operators will think:

„Biometric application must be acceptable for the users“
Acceptability

Survey in Germany - among 140 individuals

- Biometrics is widely acceptable
  "Biometric recognition based on which characteristics do you know/ accept?"

Acceptability

Survey in Germany - among 140 individuals

- Biometrics is widely acceptable
  “Have you used biometrics?”
  “Do biometrics facilitate daily life/ are they necessary?”

Mobile Biometrics
Foreground authentication (user interaction)

- Deliberate decision to capture (willful act)
- **Camera-Sensor**
  - Fingerprint recognition
    - Apples iPhone 5S / Samsung Galaxy 5
    - Fingerphoto analysis
  - Face recognition
  - Iris recognition
- Touchpad: allows signature recognition

Background authentication (observation of the user)

- Microphone
  - Speaker recognition
- Accelerometer
  - Gait recognition
  - concurrent - unobtrusive
Smartphone Access Control - with PAD

Capture process

- Camera operating in macro modus

Preview image of the camera with LED on (left) and LED off (right)

- LED permanent on

Finger illuminated

Mobile Biometric Application - Biometric Transaction and Authentication Protocol (BTAP)
Biometric Transaction Authentication Protocol (BTAP)

1.) Shared secret
- received via subscribed letter from the bank
- entered once to the smartphone
  - hash over the secret constitutes a Pseudonymous Identifier (PI)

2.) Biometric enrolment
- Biometric samples are captured

PIN = 4768

CodeBookVector (CBV)

ReferenceBinayVector (RBV)
Biometric Transaction Authentication Protocol (BTAP)

3.) Secure storage of auxiliary data

- we neither store the confidential secret nor the sensitive biometric data (i.e. feature vector)
- the secret and biometric data are merged

Auxiliary data (AD) stored in the Smartphone
- Biometric Transaction Device = FIDO Authenticator
1. Operations of the Online-Banking-Software (BSW)

- Customer generates by interacting with the BSW-Software a new Transaction-Order-Record (TOR)

This TOR consist of:

- Transaction-Identifier (TID), Sender-Account-Number (SAN)
- Receiver-Account-Number (IBAN), Ordered Amount (ORA)

- BSW transfers TOR to the Online-Banking-Server (OBS)

- BSW transfers TOR to Smartphone (BTD / FIDO Authenticator)
BTAP - Transaction

2. Operations on the Smartphone (BTD)

- **Approval** of the intended transaction by capturing a probe sample
- A secret vector $CBV'$ is reconstructed with XOR operation from the Auxilliary Data $AD$ that was stored in the BTD and from the binarized feature vector $XBV$
Key features of BTAP

- independent **two channel** verification
- **reconstruction** of shared secret
- the Pseudonymous Identifier (PI) constitutes a seal
- **seal operation** over the TOR to authenticate the transaction
Conclusion

Biometrics is possible with today’s smartphones

- a multi-biometric authentication scheme with scaling factors is a good choice with respect to security threats

Biometric standards are available

- financial transaction schemes should follow technical standards
- financial transaction schemes should follow privacy standards

BTAP follows the two channel concept

- is based on international ISO/IEC standards
- is privacy friendly as no biometric reference is stored on a banking server

More and detailed information on BTAP at:
http://www.christoph-busch.de/projects-btap.html