Biometric Recognition –
Myths dispelled and Best Practices

Christoph Busch
CRISP / European Association for Biometrics / NTNU
http://www.christoph-busch.de

Biometrics in Finance
Frankfurt - December 07  2018
Agenda

• The foundation of biometrics
• From Biometric Myths to Reality
• Mobile Biometrics
• Standards
• A Privacy Compliant Biometric Payment Protocol
• Some thoughts on Artificial Intelligence
Introduction to Biometrics
Access Control

Traditionally we place between

- individuals
- and objects
- a token (i.e. key)
Access Control

But in reality individuals
- do not have just one
- but many keys
- granting access to many doors
Access Control

In addition I have

- a Campus Card and many others
- granting access to many doors
Access Control

For some individuals

- the collection of cards is quite impressive and inconvenient
Identity authentication can be achieved by:

- **Something you know:**
  Password, PIN, other secret

- **Something you own:**
  SmartCard, USB-token, key

- **Something you are:**
  Body characteristics

Something you know or own you may lose, forget or forward to someone else, with biometrics this is more difficult.
International Organization for Standardization defines:

- **Biometrics:**
  
  "automated recognition of individuals based on their behavioural and biological characteristics"

- Remark: **behavioural** has to do with the function of the body, **biological / anatomical** has to do with the structure of the body.
Biometrics - Process

Data Subject

Capture Device

Sample

Features

Reference

Characteristic

Sample

Features Reference

Comparison

Similarity Score

Capture Device

Characteristics

Sample

Features

Reference

Comparison

Similarity Score
Biometrics - Tomorrow

it won‘t take long

- and NFC enabled Smart Phones will open most of our doors
Biometric Myths Dispelled
Security?

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“
We need to protect biometric reference data! but …

- how to **revoke** biometric references?
- how to **protect sensitive information** in biometric data?
  - and align with the General Data Protection Regulation (GDPR)

Wart Fingerprint  
Source: TU Brno, 2013
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.
  - **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


Biometric Template Protection

Protection at the same accuracy level is possible

- Bloom filter-based pseudonymous identifiers

Bloom Filter-based transformation of biometric templates

Protected Template

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:


ISO/IEC 24745
Biometric Information Protection !
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
Biometric Performance Testing

ISO/IEC 19795-1: Biometric performance testing and reporting
Part 1: Principles & Framework

- Technology testing
  - Algorithmic level verification error
    - False-Match-Rate (FMR) - algorithm accepts „zero-effort“ impostor
    - False-Non-Match-Rate (FNMR) - algorithm rejects true identity

- Scenario testing and operational testing
  - System level verification error
    - False-Accept-Rate (FAR)
    - False-Reject-Rate (FRR)
  - System level error requires observation of:
    - Sample generation: Failure-to-Capture (FTC)
    - Enrolment: Failure-to-Enrol (FTE) - no reference for this subject
    - Verification: Failure-to-Acquire (FTA) - no probe feature vector
Biometric Performance Testing - Report

DET curve (detection error trade-off curve)

- which plots error rates on both axes (false positives on the x-axis and false negatives on the y-axis)

- Extensive test results: [http://www.nist.gov/itl/iad/ig](http://www.nist.gov/itl/iad/ig)
Your Operator Reality Check

Operators should ask the vendors

• Is the sensor replaceable and robust for presentation attacks?

> I want the biometric capture device to be operated via BioAPI interface according ISO/IEC 19784 and tested for PAD according ISO/IEC 30107-3

• Can comparison algorithms be replaced?

> I want the biometric reference data to be stored in standardised interchange format according ISO/IEC 19794!

• Is the accuracy of the algorithm good?

> I want to see the technology performance test report with a DET curve according ISO/IEC 19795!

• Is there data protection of stored biometric reference data?

> I want the design of the systems to be compliant to ISO/IEC 24745
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
Mobile Biometric Payment - 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
Biometric Transaction Authentication Protocol (BTAP)

3.) Secure storage of auxilliary 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
BTAP - Transaction

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 Auxiliary Data $AD$ that was stored in the BTD and from the binarized feature vector $XBV$

```
<table>
<thead>
<tr>
<th>Reference in BTD-Storage</th>
<th>XOR</th>
</tr>
</thead>
<tbody>
<tr>
<td>10001110</td>
<td></td>
</tr>
<tr>
<td>00011000</td>
<td></td>
</tr>
<tr>
<td>10001110</td>
<td></td>
</tr>
<tr>
<td>10010110</td>
<td>XOR</td>
</tr>
</tbody>
</table>
```

$CBV'$
Transaction-Verification

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
Transaction-Verification

BTAP-Video

- http://christoph-busch.de/files/BTAP.mp4
The classical approach with texture analysis

- Image descriptors as **hand-crafted** features

```
Face
pre-processing and
feature extraction
classifier
(accept)
(reject)
```

Image Descriptors:
- LBP
- BSIF
- Sharpness
- HOG
- SIFT/SURF
- PRNU

Classifier
Morphing Attack Detection (MAD) with texture analysis

- Image descriptors as Deep features
Morphing Attack Detection (MAD) with texture analysis

- Image descriptors as Deep features
Conclusion

Biometrics is possible with today's smartphones

Biometric standards are available

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

BTAP satisfies PSD2 and 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
Contact

Contact:

Prof. Dr. Christoph Busch

Norwegian University of Science and Technology
Department of Information Security and Communication Technology
Teknologiveien 22
2802 Gjøvik, Norway
Email: christoph.busch@ntnu.no
Phone: +47-611-35-194
References - General

Web

- U.S. NIST https://www.nist.gov/topics/biometrics
- European Association for Biometrics http://www.eab.org
- da/sec biometric research group https://www.dasec.h-da.de/
- TeleTrusT working group on Biometrics
  http://www.christoph-busch.de/about-ag-biometrie.html
- Norwegian Biometrics Laboratory (NBL)
  http://www.ntnu.edu/nbl
- ISO/IEC JTC1 SC37 Working Group 3
  http://isotc.iso.org/livelink/livelink/open/jtc1sc37wg3
  http://www.christoph-busch.de/standards-sc37wg3.html
References

Complementary reading

- ISO/IEC SC37 SD11, “General biometric system architecture”, 2010
  http://isotc.iso.org/livelink/livelink?func=ll&objId=8755976&objAction=Open
  http://www.christoph-busch.de/standards.html
Complementary reading - interchange formats

References

Complementary reading - quality


Complementary reading - protection, PAD and mobile


Presentation Attack Detection - Framework

ISO/IEC 30107-1

• now freely available in the ISO-Portal


Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).
Presentation Attack Detection


- **presentation attack**
  presentation to the biometric capture subsystem with the goal of interfering with the operation of the biometric system

- **presentation attack detection (PAD)**
  automated determination of a presentation attack

Definitions in ISO/IEC 2382-37: Vocabulary
http://www.christoph-busch.de/standards.html

- **impostor**
  subversive biometric capture subject who attempts to being matched to someone else's biometric reference

- **identity concealer**
  subversive biometric capture subject who attempts to avoid being matched to their own biometric reference
Presentation Attack Detection

Impostor

- impersonation attack
  - positive access 1:1 (two factor application)
  - positive access 1:N (single factor application)
- finding a look-a-like
- making appearance similar to the reference
- artefact presentation

Concealer

- evasion from recognition
  - negative 1:N identification (watchlist application)
- depart from standard pose
- evade face detection

Image Source: http://upshout.net/game-of-thrones-make-up
Image Source: https://cvdazzle.com
Image Source: https://www.youtube.com/watch?v=LRj8whKmN1M
ISO/IEC 30107-1 - 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

(General Noun)

(Adjectives describing categories)

(Qualifying adjectives)
Definition of full system vulnerability metric w.r.t. attacks

- **Impostor attack presentation match rate (IAPMR)**
  
  *in a full-system evaluation of a verification system* the proportion of impostor attack presentation using the same PAI species in which the target reference is matched

Source: ISO/IEC 30107-3

- **Concealer attack presentation non-match rate (CAPNMR)**
  
  in a full-system evaluation of a verification system, the proportion of concealer attack presentations using the same PAI species in which the target reference is not matched.

Source: ISO/IEC 30107-3
Definition of detection capabilities metrics

- Testing the PAD subsystem with false-negative and false-positive errors:
  
- **Attack presentation classification error rate (APCER)**
  proportion of *attack presentations using the same PAI species incorrectly classified as bona fide presentations in a specific scenario*

- **Bona fide presentation classification error rate (BPCER)**
  proportion of *bona fide presentations incorrectly classified as attack presentations in a specific scenario*

Source: ISO/IEC 30107-3
Definition of PAD metrics elements

- **PAI species**
  
  *class of presentation attack instruments created using a common production method and based on different biometric characteristic*

- **Attack potential**
  
  *measure of the capability to attack a TOE given the attacker’s knowledge, proficiency, resources and motivation*

- **target of evaluation (TOE)**
  
  *within Common Criteria, the IT product that is the subject of the evaluation*

Source: ISO/IEC 30107-3
Definition of detection capabilities metrics

- Testing the PAD subsystem with false-negative errors:

- **Attack presentation classification error rate (APCER)**
  proportion of *attack presentations* using the same PAI species incorrectly *classified as bona fide presentations* in a specific scenario

\[
APCER_{PAIS} = 1 - \left( \frac{1}{N_{PAIS}} \right) \sum_{i=1}^{N_{PAIS}} Res_i
\]

- \(N_{PAIS}\) is the number of *attack presentations* for the given PAI species
- \(Res_i\) takes value 1 if the \(i^{th}\) presentation is classified as an attack presentation, and value 0 if classified as a *bona fide presentation*

*Source: ISO/IEC 30107-3*
Definition of detection capabilities metrics

- DET curve analyzing operating points for various security measures and convenience measures

Example: