Biometrics are ready for banking: standards and security

Christoph Busch
Hochschule Darmstadt / Gjøvik University College
http://www.christoph-busch.de/

EAB / FFAUK / BdB / EPCA - Biometrics in Banking

London - October 24, 2014
Agenda

• From Biometric Rumors to Reality
• Mobile Biometrics
• Mobile Payment Protocol
  - Privacy compliant protocol according to the FIDO Universal Authentication Framework (UAF)
  - a suggestion for a „European derivate of Apple Pay“
Answers on Biometric Rumors
Security?

Operators may think:

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

1. **Tragedy of the commons**
   - The concept works well when we have to manage only a few passwords.
   - But in reality, we are expected to remember more than 100 passwords and we fail to do so.

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

• 2.) 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 $H = L \times \log_2 N$
  - The entropy is limited to less than **20bit** (with $L=6, N=10$)

  - The reported entropy for different biometric characteristics is
    - Fingerprints **84bit** [Ratha2001]
    - Iris **249bits** [Daugman2006]
    - Face **56bit** [Adler2006]

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

3.) 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!
Data subjects *may* think:

„The number of biometric characteristics is *limited* (e.g. we have only 10 fingers) - we can not revoke the biometric *reference*“
Variation of Biometric Measurement?

Operators may think:

„There is a strong variance in biometric measurements“
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.
  - **Noise-robustness**: Stored information can be used for authentication with noisy biometric samples
  - **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 Privacy and Data Protection?

Operators may think:

„Biometric systems are not compliant to data privacy principles“
Requirements for data privacy and data protection are formulated in:

- Directive 95/46/EC: On the protection of individuals with regard to the processing of personal data and on the free movement of such data

- EU data protection regulation under development - since 2012

- Regulation 45/2001: on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data

- Directive 2002/58/EC: concerning the processing of personal data and the protection of privacy in the electronic communications sector
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 !**
Operators may think:

“Biometric sensors can not detect gummy and cut-off fingers”
Presentation Attack Detection

Attacks on capture devices

- ISO/IEC 30107 Presentation Attack Detection
  - aka spoof detection

Countermeasures

- Vein recognition
- Fingerphoto recognition
- Fingerprint Recognition with Optical Coherence Tomography (OCT)
  - current research topic
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
The 19794-Family: Biometric data interchange formats
the semantic is equivalent for binary encoded and XML encoded records
Your Operator Reality Check

Operators should ask the vendors

- Is there a vendor lock-in due to proprietary sensors?
  
  *I want the biometric capture device to be operated via BioAPI interface according ISO/IEC 19784!*

- 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 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 (wilful 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
Biometric Gait Recognition

Offer an unobtrusive authentication method

- Use accelerometers - already embedded in mobile devices to record the gait
  - No extra hardware is necessary
  - Acceleration measured in 3-directions

- First paper on this topic:
Biometric Gait Recognition

Data capture process

- periodical pattern in the recorded signal

![Graph showing acceleration over time with labels for different phases of gait cycle.]

Best result

- now at 6.1% Equal-Error-Rate (EER)
Capture process

- Camera operating in \textit{macro} modus

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

- LED permanent on

Finger illuminated

Finger recognition study - 2012/2013

• Result: biometric performance at 1.2% EER

Mobile Biometric Payment - Biometric Transaction and Authentication Protocol (BTAP)
Elements in the Online-Banking-Scenario:
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)**

<table>
<thead>
<tr>
<th>PIN-Letter</th>
<th>Deutsche Post</th>
<th>Lilli Muster</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Online-Bank</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Server-Alle-24</td>
<td></td>
</tr>
<tr>
<td></td>
<td>61004 Frankfurt</td>
<td>Main</td>
</tr>
<tr>
<td></td>
<td>IBAN: 500 703 40</td>
<td>4711 123456</td>
</tr>
</tbody>
</table>

PIN = 4768

2.) Biometric enrolment
- Biometric samples are captured

**CodeBookVector (CBV)**

**ReferenceBinayVector (RBV)**
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

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

This TOR consist of:

- Bankleitzahl: 500 403 40
- Kontonummer: 4538

- **ORA**: 2.9 Mio EURO
- **RAN**: 500 403 40

- **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 $XBV$
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 todays smartphones

- a biometric authentication factor 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
Contact

Prof. Dr. Christoph Busch
Principal Investigator
CASED
Mornewegstr. 32
64293 Darmstadt/Germany
christoph.busch@cased.de
+49 6151/16 9444
www.cased.de
Contact

Christoph Busch, Dr.-Ing.
Professor

P.O. Box 191, N-2802 Gjøvik, Norway
Phone: +47 61 13 51 94
Fax: +47 61 13 52 40
E-mail: christoph.busch@hig.no
www.hig.no | www.nislab.no