BTAP: Secure Authentication of Banking Transaction data using biometric Identifiers

Christoph Busch
European Association for Biometrics / Fraunhofer IGD
http://www.christoph-busch.de/about-talks-slides.html

Biometrics in Banking and Payments
London - October 16, 2015
Agenda

- Mobile biometrics
- Requirements for secure and reliable biometrics
- Biometric Transaction Authentication Protocol (BTAP)
  - a proposal for a „European derivate of Apple Pay“
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

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

Finger recognition study - 2012/2013

- Result: biometric performance at 1.2% EER

Biometric Eye Recognition

Images captured with either front or back camera

• Challenges
  - face and eye localization
  - feature extraction with SURF, SIFT und Binarized Statistical Image Features (BSIF)


Biometric Face and Eye Recognition

Multimodal Fusion
### Multimodal Fusion - Biometric Performance

<table>
<thead>
<tr>
<th>Fusion Scheme</th>
<th>Camera</th>
<th>Samsung S5</th>
<th>Samsung Note</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>GMR@FMR=0.01%</td>
<td>EER</td>
</tr>
<tr>
<td>Min Rule</td>
<td>Back Assisted</td>
<td>99.17</td>
<td>0.43</td>
</tr>
<tr>
<td></td>
<td>Back</td>
<td>97.12</td>
<td>0.93</td>
</tr>
<tr>
<td>Max Rule</td>
<td>Back Assisted</td>
<td>50.78</td>
<td>10.71</td>
</tr>
<tr>
<td></td>
<td>Back</td>
<td>52.94</td>
<td>12.10</td>
</tr>
<tr>
<td>Product</td>
<td>Back Assisted</td>
<td>84.13</td>
<td>15.34</td>
</tr>
<tr>
<td></td>
<td>Back</td>
<td>84.81</td>
<td>14.37</td>
</tr>
<tr>
<td>Weighted Fusion</td>
<td>Back Assisted</td>
<td>99.13</td>
<td>0.43</td>
</tr>
<tr>
<td></td>
<td>Back</td>
<td>97.98</td>
<td>0.68</td>
</tr>
</tbody>
</table>

Requirements
Balance the Requirements

The requirements from operators / end-user
Balance the Requirements

The requirements from operators / end-user

- Convenience
- Privacy Protection
- Security
Convenience ?

Operators will think:

„The biometric transactions system must be convenient for the end-user“
Establish biometrics in the known environment

- No extra costs
- No extra training

Image Source: Apple 2013
Operators will think:

„The biometric sensors must be robust against fake attacks“
Security?

- Presentation Attacks
Gummy Finger Production in 2000!

Attack **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 circuit board mold
Gummy Finger Production in 2000!

Reported in a publication by the German Federal Police

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

- **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*
Definition of harmonized metrics in ISO/IEC 30107-3

- **Attack presentation classification error rate (APCER)**
  proportion of *attack presentations* incorrectly classified as *normal presentations* at the component level in a specific scenario

- **Normal presentation classification error rate (NPCER)**
  proportion of *normal presentations* incorrectly classified as *attack presentations* at the component level in a specific scenario
Eye recognition study - 2015

- Presentation Attack Detection (PAD) videos on iPhone 5 S and Nokia 1020

- Method based on Eulerian Video Magnification (EVM)
  - Normalized Cumulative Phase Information

- Zero Error Rates:
  - APCER = 0 %
  - NPCER = 0 %

Privacy Protection ?

Operators will think:

„Biometric systems must be compliant to data privacy and data protection principles“
Data Protection Requirements

Technical framework on how to implement requirements for data privacy and data protection

• exists ISO/IEC 24745: Biometric Information Protection, (2011)
Why multiple Modalities?
Financial Transactions

- Position of the Bundesverband Deutscher Banken (BdB)
  - number and strength of biometric factors should **scale** with transaction volume


Image Source: BdB 2015
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 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
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 $XBV$
BTAP - Transaction

2. ) Operations of the Biometric-Transaction-Device (BTD)

- The relevant Information of the Transaction-Order-Record (TOR) is visualized in the display of the BTD:
  - Receiver-Account-Number (RAN), Ordered Amount (ORA)
- Approval of the intended transaction by probe sample
- Auxilliary Data $ADI_{(0,1,2,4,5,8,11,12)}$ is extracted from BTD-storage
- A binarized feature vector $XBV$ is reconstructed
- A secret vector $CBV'$ is reconstructed
- The secret key $SBV'$ is freshly re-computed from $CBV'$
  \[ SBV' = \text{dec} (CBV') \]
2.b ) Mirror-Operations of the BTD and the OBS

- A Transaction-Order-Seal (TOS‘) is computed
  - of the Transaction-Order-Record \( TOR \)
  - and the reconstructed secret key \( SBV‘ \)

\[
TOS' = MAC \left( h(TOR), h(SBV') \right)
\]

- The seal (TOS‘) is transferred to the Online-Banking-Server
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
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
Kontakt

Prof. Dr. Christoph Busch

Fraunhoferstrasse 5
64283 Darmstadt, Germany
Phone: +49-6151-155-536
christoph.busch@igd.fraunhofer.de
www.igd.fraunhofer.de/~busch