Security Evaluation of Vascular Biometrics

4th May, 2016.

Akira Otsuka, Tetsushi Ohki
AIST, Japan
How to evaluate the Security of Biometrics

Common Criteria

• 5 levels of Attack Potential (AP)
  Basic, Enhanced-Basic, Moderate, High, Beyond High

• Tester makes the best efforts to attack the TOE
  If no attack is found within the given AP,
  TOE is considered secure against any attack below AP.

ISO/IEC 30107, “Biometric Presentation Attack Detection”

• Attack Presentation Classification Error Rate

\[
APCER_{AP} = \max_{PAIS \in \mathcal{A}^A} \frac{1}{N_{PAIS}} \sum_{i=1}^{N_{PAIS}} (1 - Res_i)
\]

PAIS: Presentation Attack Instrument Species
\( \mathcal{A}_{AP} \): a subset of PAI species with attack potential at or below AP
Relation between AP and APCER(1)

Case 1: Enhanced Basic

Acceptable Successful Presentation Attack Probability for CC (Assumed)
Relation between AP and APCER(2)

Case 2: Below Basic

Acceptable Successful Presentation Attack Probability for CC (Assumed)
A Gap between Theory and Practice

Realistic Case: Effective Presentation Attack NEVER FOUND
Is this Secure?

Exhaustive Test

Gap

Acceptable Successful Presentation Attack Probability for CC (Assumed)

Best Effort Test

APCER (%) vs AP(Score)

5 10 15 20 25 30

Basic Enhanced Basic Moderate High Beyond High

APCER
How to close the GAP?

**Sensor-independent Security Evaluation**

- Same test set can apply many TOE’s (Ideally)
- That’s good, but…
  - “Universal“ attack instruments (applicable to many TOE’s) are hard to produce in many cases
    — Palm vein vs Finger vein / Front vs Side finger vein

**Sensor-dependent Security Evaluation**

- Provide (as much as possible) internal specification of TOE to test labs. Test labs will create(or provided) Simulated Sensor/Algorithm:
  - Sensor Specification — **Simulated Sensor**
  - Algorithm Specification — **Simulated Algorithm**
- Create “**good attack instruments**” based on simulated sensor.
Variety of Vascular Biometrics

(I) Palm Vein Scanner
Reflective

(II) Font Finger Vein Scanner
Direct Transmissive

(III) Side Finger Vein Scanner
Reflective

(IV) Front Finger Vein Scanner
Indirect Transmissive
Sensor-dependent Security Evaluation

\{\alpha_1, \alpha_2, \ldots, \alpha_n\}:\text{ Presentation Attack Instruments (PAI) species}

PAI species \(\alpha_i\) is indistinguishable from Bona Fide presentation by a sensor if and only if

\[\text{APCER}_{\alpha_i} + \text{BPCER} \approx 1\]

**Divide and Conquer**

In a case TOE consists of …

- NIR Image Sensor
- Conductive Sensor
- Blood Flow Sensor

**Arithmetics on Indistinguishable Sets**

Set of PAIs on each sensor narrows down the set of PAI on TOE

\[A_{\text{TOE}} \supseteq A_{\text{NIR}} \cap A_{\text{Cond}} \cap A_{\text{Blood}}\]
Sensor-dependent Security Evaluation

1. Acquire internal specification of TOE
2. Create Simulated Sensor A (Simulated algorithm A)
3. Search for Indistinguishable PAI for Simulated Sensor A
4. Combine PAI A and B
5. Conduct Presentation Attack on TOE
6. Compute APCER<sub>AP</sub>

Skip if sensor is provided by the vendor or commercially available.

If multiple sensors are identified...

Vulnerability Assessment Process
Preliminary Experiment

**Example TOE**

![Image of a custom designed capturing device](Image-293x329)

**Simulated Sensor**

![Image of a Raspberry Pi2 board with a custom designed capturing device](Image-233x84)

**[TV13] Finger Vein Sensor**


<table>
<thead>
<tr>
<th>Example TOE</th>
<th>Simulated Sensor</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Image Sensor</strong></td>
<td>C-Cam Tech. BCi5 1280x1024</td>
</tr>
<tr>
<td><strong>NIR Filter</strong></td>
<td>B+W 093 IR filter 800nm - 930nm band-pass filter</td>
</tr>
<tr>
<td><strong>Light Source</strong></td>
<td>850nm Oslam SFH4550 x 8 LED Adaptive Intensity Control</td>
</tr>
<tr>
<td><strong>Algorithm</strong></td>
<td>bob.fingervein*</td>
</tr>
</tbody>
</table>

*) idiap, available at [https://github.com/biidiap/bob.fingervein](https://github.com/biidiap/bob.fingervein)
Quality Control of Fake Samples

Control: Improve Sensor and Fake Production until Fake is indistinguishable from Live on the Simulated Sensor

\[ \text{APCER}_{\text{FAKE}} + \text{BPCER}_{\text{LIVE}} \approx 1 \]
Fake Production

(A) Paper / Histogram Equalization

(B) OHP / Histogram Equalization

(C) Paper / PSF Deconvolution

(D) OHP / PSF Deconvolution

Material / Image Process

OHP /  Histogram Equalization
Thick Paper / PSF Deconvolution

Live Sample

Live-02-L-1.jpg
## Preliminary Experiment

<table>
<thead>
<tr>
<th>Biometric Samples</th>
<th>Sensor</th>
<th>Original NIR Sensor (Type II: Front Transmissive Vein Scanner)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Subjects</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>Number of Samples</td>
<td>Left and Right Index Finger x 8 samples each 1 as Gallery, 7 for Probe</td>
<td></td>
</tr>
</tbody>
</table>

### Spoof Production

<table>
<thead>
<tr>
<th>Material</th>
<th>OHP (for Laser Printer), Thick Paper (Thickness 175μm, Weight 158g/m²)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Image Enhancement</td>
<td>CLAHE (Contrast Limited Adaptive Histogram Equalization), PSF Deconvolution (Wiener Deconvolution of Point Spread Func.)</td>
</tr>
</tbody>
</table>

### Verification

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>bob.fingervein (Algorithm [Miura2005])</th>
</tr>
</thead>
</table>
| Verification Count | Live-Live Genuine: 224 pairs  
Live-Live Imposter: 768 pairs  
Fake-Live Genuine: 224 pairs |
Preliminary Experiment Result

(A) OHP / Histogram Equalization

APCER = 16%

(B) Thick Paper / Histogram Equalization

APCER = 36%

(C) OHP / PSF Deconvolution

APCER = 0%

(D) Thick Paper / PSF Deconvolution

APCER = 0%
Conclusion

• In **Sensor-independent Security Evaluation** (Toolkit),
  • “Universal“ presentation attack instruments (applicable to many sensors) are hard to produce especially in vascular biometrics.

• Introduced **Sensor-dependent Security Evaluation**
  Test labs are provided (as much as possible) internal specification of TOE.
  Test labs will create(or provided) **Simulated Sensor/Algorithm**

  • **Quality control** of Presentation Attack Instruments
  • **Narrow down** the (infinitely many) set of PAIs to the (small) set of the most effective PAIs.

• Shown the preliminary experimental results
  • **Quality measurement** improves the quality of PAIs.