Biometrics and (IT) Security

Axel Munde

German Federal Office for Information Security
Motivation

Actual situation of biometrics in governmental environment

• Issuing of biometric enabled Passports and ID Cards (Face only (38%) and Finger (62%)) in 94 states worldwide

• About 360 millions of ePassports / (ID Cards) are issued

• Increasing use of biometrics in border control (16 states using ABC)

• 30 ICAO participating states

• Mandatory taking fingerprints for applying for a Schengen Visa / European Union

Numbers published by US State Department in Sept. 2011
Motivation

- Increasing numbers of passengers
- Assured transfer time of passenger – Economic factor for airport operating companies
- Mandatory biometric usage for Schengen Visa

Question?

Why not use biometrics for ePassport (verification) and Visa (identification) in a self service environment for border control and visa request? (Increasing national security and speeding up processes)
Content

• Biometrics and (IT) Security / Faking Biometrics (Fingerprint)

• Common Criteria
  – Structure
  – Security functional and Assurance classes
  – Evaluation Assurance Level (EAL)
  – Biometric Protection Profiles
  – Attack potential and Examples (Fake detection)

• Methodologies for evaluation of fake detection (Fingerprint)

• Summary
Biometric characteristic (refined from SC37HBV)
Biological or behavioural characteristic of an individual that can be detected and from which distinguishing, repeatable biometric features can be extracted for the purpose of automated recognition of individuals (e.g. fingerprint)

⇒ Biometrics is a (IT) means to ensure the „identity“ of user

⇒ Has to fulfill the „traditional“ IT (security) requirements
Challenges of Biometrics

1. FAR / FRR – Statistical properties (BEM <=> SC37 WG5 Standards)
2. Strong and weak biometrics and the “Zoo” (User depending) – Quality related?
   1. and 2. – No (technical) tools used for attacking
3. Attacks on biometric systems using fakes

⇒ In the following only direct attacks, using faked biometrics (limited to fingerprints).
⇒ Are **Common Criteria** (CC) adequate to address the security challenges?
Producing Fakes

Digitizing, enhancing and modifying

Raw finger image

Printing

wood glue

http://dasalte.ccc.de/biometrie/fingerabdruck_kopieren?language=de
http://dasalte.ccc.de/biometrie/fingerabdruck_kopieren?language=en

“Wie können Fingerabdrücke nachgebildet werden? 09. Oktober 2004 (starbug)“
“The trust in biometric systems depends on their reliability AND their level of security!”

There are many types of publicly known fakes … and a wide range of variations

With little experience fakes are:
made of cheap & easy obtainable materials
relatively easy to produce
able to deliver high quality fingerprints
adaptable by additives like: magnetic powder, color…

The challenge for spoof detection is to distinguish between all existing human fingers and all possible spoofing material
Common Criteria in a Nutshell

2009: Common Criteria
Version 3.1
Release 3
ISO/IEC 15408:2009

Homepage: www.commoncriteriaportal.org
Common Criteria (V 3.1) - Structure

- Consists of 3 or 4 parts:
  - **Part 1**: Introduction and general model
  - **Part 2**: Security functional components
  - **Part 3**: Security assurance components

- Instructions for the evaluation are given by the Common Evaluation Methodology (CEM) (Part 4)

- Protection Profile (PP) – Implementation independent description of a TOE type

- Security Target (ST) – Implementation dependent description of a specific TOE – Could base on evaluated PP
Common Criteria (V 3.1) - Evaluation

- Evaluated will be **Security Target, configuration management, delivery procedures, design documentation, guidance documentation** as well as **development and production sites**

- Product testing and vulnerability analysis

- Evaluation is structured in 7 level, so-called Evaluation Assurance Level, short EAL-Level (Assurance Packages)

- Raised depth of evaluation (trust) from EAL 1 – 7

- Raised requirements for documentation, development and production sites, intensity of the evaluation and resistance against attackers
Common Criteria (V 3.1) – EAL Level

EAL1 - functional tested
EAL2 - structural tested
EAL3 - methodical tested and checked
EAL4 - methodical designed, tested, and reviewed
Up to EAL4 international mutual recognition of evaluation (CCRA)
EAL5 - semiformal designed and tested
EAL6 - semiformal verified design and tested
EAL7 - formal verified design and tested
Common Criteria (V 3.1) – Part 2
Security Classes

- CLASS FAU: SECURITY AUDIT
- CLASS FCO: COMMUNICATION
- CLASS FCS: CRYPTOGRAPHIC SUPPORT
- CLASS FDP: USER DATA PROTECTION
- CLASS FIA: IDENTIFICATION AND AUTHENTICATION
- CLASS FMT: SECURITY MANAGEMENT
- CLASS FPR: PRIVACY
- CLASS FPT: PROTECTION OF THE T(OE) S(ecurity) F(unction)
- CLASS FRU: RESOURCE UTILISATION
- CLASS FTA: TOE ACCESS
- CLASS FTP: TRUSTED PATH/CHANNELS
Common Criteria (V 3.1) - Part 3
Assurance Classes

- CLASS APE: PROTECTION PROFILE EVALUATION
- CLASS ASE: SECURITY TARGET EVALUATION
- CLASS ADV: DEVELOPMENT
- CLASS AGD: GUIDANCE DOCUMENTS
- CLASS ALC: LIFE-CYCLE SUPPORT
- CLASS ATE: TESTS
- CLASS AVA: VULNERABILITY ASSESSMENT
- CLASS ACO: COMPOSITION
<table>
<thead>
<tr>
<th>Assurance class</th>
<th>Assurance Family</th>
<th>Assurance Components by Evaluation Assurance Level</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>EAL1</td>
</tr>
<tr>
<td>Development</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ADV_ARC</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>ADV_FSP</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>ADV_IMP</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>ADV_INT</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>ADV_SPM</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ADV_TDS</td>
<td>1</td>
</tr>
<tr>
<td>Guidance documents</td>
<td>AGD_OPE</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>AGD_PRE</td>
<td>1</td>
</tr>
<tr>
<td>Life-cycle support</td>
<td>ALC_CMC</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>ALC_CMS</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>ALC_DEL</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>ALC_DVS</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>ALC_FLR</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ALC_LCD</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>ALC_TAT</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Target evaluation</td>
<td>ASE_CCL</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>ASE_ECD</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>ASE_INT</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>ASE_OBJ</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>ASE_REQ</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>ASE_SPD</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>ASE_TSS</td>
<td>1</td>
</tr>
<tr>
<td>Tests</td>
<td>ATE_COV</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>ATE_DPT</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ATE_FUN</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>ATE_IND</td>
<td>1</td>
</tr>
<tr>
<td>Vulnerability assessment</td>
<td>AVA_VAN</td>
<td>1</td>
</tr>
</tbody>
</table>
Biometric Protection Profiles – An Overview

   http://www.niap-ccevs.org/pp/PP_BVM_BR_V1.0/
   Date: 12 January 2006 – Common Criteria Version: 2.3

   Not assigned to any Validated Products

   Date: 25 July 2007 – Common Criteria Version: 2.3

   Not assigned to any Validated Products
3. **Biometric Device Protection Profile (BDPP)**
   **Date:** 5. September 2001 – Common Criteria Version: 2.3
   Ever used?

4. **Biometric Verification Mechanisms Protection Profile Version 1.3**
   (BSI-CC-PP-0043-2008) – Evaluated PP
   https://www.bsi.bund.de/ContentBSI/Themen/ZertifizierungundAnerkennung/ZertifierungnachCCundITSEC/SchutzprofileProtectionProfile/schutzprofile.html#P0016
   **Date:** 07. August 2008 – Common Criteria Version: 3.1 Rev 2

5. **Protection Profile - Biometric Verification Mechanisms Version 1.04**
   (BSI-PP-0016-2005) – Evaluated PP
   https://www.bsi.bund.de/ContentBSI/Themen/ZertifizierungundAnerkennung/ZertifierungnachCCundITSEC/SchutzprofileProtectionProfile/schutzprofile.html#P0016
   **Date:** 17. August 2005 – Common Criteria Version: 2.3
   Based on PP 1. - 3. – Used for 2 Products – 1 under re-evaluation
6. **Fingerprint Spoof Detection Protection Profile (FSDPP), Version 1.8**  
(BSI-CC-PP-0063-2010)  
ePP/pp0063b_pdf.pdf?__blob=publicationFile  
**Date:** 23\textsuperscript{th} November, 2009 – Common Criteria Version: 3.1 Rev 3  
2 Products under evaluation

7. **Fingerprint Spoof Detection Protection Profile based on Organisational Security Policies (FSDPP\_OSP), Version 1.7**  
(BSI-CC-PP-0062-2010)  
ePP/pp0062b_pdf.pdf?__blob=publicationFile  
**Date:** 27\textsuperscript{th} November 2009 – Common Criteria Version: 3.1 Rev 3
### How to calculate Attack Potential

**Elapsed Time**

<table>
<thead>
<tr>
<th>Elapsed Time</th>
<th>Factor Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;= one day</td>
<td>0</td>
</tr>
<tr>
<td>&lt;= one week</td>
<td>1</td>
</tr>
<tr>
<td>&lt;= two weeks</td>
<td>2</td>
</tr>
<tr>
<td>&lt;= one month</td>
<td>4</td>
</tr>
<tr>
<td>&lt;= two months</td>
<td>7</td>
</tr>
<tr>
<td>&lt;= three months</td>
<td>10</td>
</tr>
<tr>
<td>&lt;= four months</td>
<td>13</td>
</tr>
<tr>
<td>&lt;= five months</td>
<td>15</td>
</tr>
<tr>
<td>&lt;= six months</td>
<td>17</td>
</tr>
<tr>
<td>&gt; six months</td>
<td>19</td>
</tr>
</tbody>
</table>
How to calculate Attack Potential
- *Expertise* and *Knowledge of TOE* -

<table>
<thead>
<tr>
<th>Expertise</th>
<th>Factor Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Layman</td>
<td>0</td>
</tr>
<tr>
<td>Proficient</td>
<td>3(^{(1)})</td>
</tr>
<tr>
<td>Expert</td>
<td>6</td>
</tr>
<tr>
<td>Multiple experts</td>
<td>8</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Knowledge of TOE</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Public</td>
<td>0</td>
</tr>
<tr>
<td>Restricted</td>
<td>3</td>
</tr>
<tr>
<td>Sensitive</td>
<td>7</td>
</tr>
<tr>
<td>Critical</td>
<td>11</td>
</tr>
</tbody>
</table>

\(^{(1)}\) When several proficient persons are required to complete the attack path, the resulting level of expertise still remains “proficient” (which leads to a 3 rating).
How to calculate Attack Potential
- Window of Opportunity and Equipment-

<table>
<thead>
<tr>
<th>Window of Opportunity</th>
<th>Factor Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unnecessary / unlimited access</td>
<td>0</td>
</tr>
<tr>
<td>Easy</td>
<td>1</td>
</tr>
<tr>
<td>Moderate</td>
<td>4</td>
</tr>
<tr>
<td>Difficult</td>
<td>10</td>
</tr>
<tr>
<td>None</td>
<td>(2)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Equipment</th>
<th>Factor Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard</td>
<td>0</td>
</tr>
<tr>
<td>Specialised</td>
<td>4 (3)</td>
</tr>
<tr>
<td>Bespoke</td>
<td>7</td>
</tr>
<tr>
<td>Multiple bespoke</td>
<td>9</td>
</tr>
</tbody>
</table>

(2) Indicates that the attack path is not exploitable due to other measures in the intended operational environment of the TOE.

(3) If clearly different test benches consisting of specialised equipment are required for distinct steps of an attack, this should be rated as bespoke.
### How to calculate Attack Potential

- **The Result** -

\[
\text{Attack Potential} = \text{Elapsed Time} + \text{Expertise} + \text{Knowledge of TOE} + \text{Window of Opportunity} + \text{Equipment}
\]

<table>
<thead>
<tr>
<th>Values</th>
<th>Attack potential required to exploit scenario:</th>
<th>TOE resistant to attackers with attack potential of</th>
<th>Meets assurance components</th>
<th>Failure of components</th>
</tr>
</thead>
<tbody>
<tr>
<td>0-9</td>
<td>Basic</td>
<td>No rating</td>
<td>-</td>
<td>AVA_VAN.1 - .5</td>
</tr>
<tr>
<td>10-13</td>
<td>Enhanced-Basic</td>
<td>Basic</td>
<td>AVA_VAN.1 - .2</td>
<td>AVA_VAN.3 - .4</td>
</tr>
<tr>
<td>14-19</td>
<td>Moderate</td>
<td>Enhanced-Basic</td>
<td>AVA_VAN.1 - .3</td>
<td>AVA_VAN.4 - .5</td>
</tr>
<tr>
<td>20-24</td>
<td>High</td>
<td>Moderate</td>
<td>AVA_VAN.1 - .4</td>
<td>AVA_VAN.5</td>
</tr>
<tr>
<td>=&gt;25</td>
<td>Beyond High</td>
<td>High</td>
<td>AVA_VAN.1 - .5</td>
<td></td>
</tr>
</tbody>
</table>
**1. Example – Fingerprint System**
No fake detection; system commercial available; information in internet, unlimited access

<table>
<thead>
<tr>
<th>Elapsed Time</th>
<th>&lt;= one week</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Expertise</td>
<td>Layman</td>
<td>0</td>
</tr>
<tr>
<td>Knowledge of TOE</td>
<td>Public</td>
<td>0</td>
</tr>
<tr>
<td>Window of Opportunity</td>
<td>Unnecessary / unlimited access</td>
<td>0</td>
</tr>
<tr>
<td>Equipment</td>
<td>Standard</td>
<td>0</td>
</tr>
</tbody>
</table>

⇒ Attack potential is 1
⇒ Fails EAL1
2. Example – Fingerprint System
Fake detection; system commercial available; information in internet, limited access (Supervised)

<table>
<thead>
<tr>
<th>Elapsed Time</th>
<th>&lt;= one week</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Expertise</td>
<td>Proficient</td>
<td>3</td>
</tr>
<tr>
<td>Knowledge of TOE</td>
<td>Public</td>
<td>0</td>
</tr>
<tr>
<td>Window of Opportunity</td>
<td>Moderate</td>
<td>4</td>
</tr>
<tr>
<td>Equipment</td>
<td>Standard</td>
<td>0</td>
</tr>
</tbody>
</table>

⇒ Attack potential is 8
⇒ Fails EAL1
3. Example – Fingerprint System
Sophisticated fake detection\(^1\); system not commercial available; information not in internet, limited access (Supervised)

\[
\begin{array}{|c|c|c|}
\hline
\text{Elapsed Time} & \leq \text{one month} & 4 \\
\hline
\text{Expertise} & \text{Proficient} & 3 \\
\hline
\text{Knowledge of TOE} & \text{Restricted} & 3 \\
\hline
\text{Window of Opportunity} & \text{Moderate} & 4 \\
\hline
\text{Equipment} & \text{Standard} & 0 \\
\hline
\end{array}
\]

⇒ Attack potential is 14 (Moderate Attack Potential)
⇒ System can be evaluated up to EAL4

1) In terms of fake recognition rate
Summary of Examples

- In examples no **Brute force** and **Hill-Climbing** attacks have been taken into account.
- At the moment no fake detection available which could be CC evaluated - Fails even EAL 1.
- Fingerprint sensor can be spoofed with relatively simple fakes.
- Some sensors recognize a subset of the available fakes.
- For a sensor usually a “golden” fake could be identified that worked reproducible.
- In order to rate the performance of current and future spoof detection technologies there is a need for a comprehensive evaluation methodology.

⇒ Need to develop of “Fingerprint Spoof Detection Methodology”
Supporting Documents on Evaluation on Fake Detection (but not limited to)

1. Characterizing Attacks to Fingerprint Verification Mechanisms
   Version 2.0 – 2010
   CCDB-2008-09-002
   Date: 2010 - 12

2. Fingerprint Spoof Detection Evaluation Guidance
   Version: 2.1
   Date: 2009 – 12 - 18
Characterizing Attacks to Fingerprint Verification Mechanisms (1.)

 Provides guidance about attack methods to be considered in the evaluation of TOEs with fingerprint verification mechanisms.
 Addresses also the standardization of the security rating for this type of mechanisms and include examples for the attack rating. (Re-introduction of Exploitation and Identification of a vulnerability)

Developed by:

Spanish National Cryptologic Centre (CCN) and the Biometric Recognition Group - ATVS of the Autonomous University of Madrid (UAM).
Fingerprint Spoof Detection
Evaluation Guidance (2.)

- Introduction of “new” extended Vulnerability Component
- Based on component used in EAL2 evaluations (To ensure developers testing and vulnerability analysis)
- Requires resistance against “minimal” attack potential instead of “basic” attack potential
- Evaluations of Spoof Detection System shall always use Flaw Remediation – To update spoof detection

<table>
<thead>
<tr>
<th>Value</th>
<th>Resistant against attackers with attack potential of:</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 – 4</td>
<td>No rating</td>
</tr>
<tr>
<td>5 – 9</td>
<td><strong>Minimal</strong></td>
</tr>
<tr>
<td>10 – 13</td>
<td>Basic</td>
</tr>
<tr>
<td>14 – 19</td>
<td>Enhanced-Basic</td>
</tr>
<tr>
<td>20 – 24</td>
<td>Moderate</td>
</tr>
<tr>
<td>&gt;= 25</td>
<td>High</td>
</tr>
</tbody>
</table>
Testing methodology:

- Main focus: Examination whether spoof detection functionality is able to detect spoofed biometric characteristics with a sufficiently reliable performance.
- Determination of security relevant error rate: False Spoof Not Detect Rate (FSNDR)
- Determination using a standardized Fake-Toolbox

Vulnerability assessment:

- Addresses slight modifications to the “most effective” fakes that are used in ATE and innovative fakes adopted to the specific technology. They must not lead to changes of error rates.
- The evaluation guidance provides interpretations of the CEM work units, gives help in finding the most promising fake and gives examples for relevant attack scenarios together with example ratings.

The TOE has not to miss the maximum error rate for each fake, the “golden” fake as well, that is presented to the system.
Summary

1. Biometric systems without fake detection are failing the lowest IT security requirements
2. Using biometric systems without security properties, the possible attacks by fakes have to be addressed by organizational means
3. First steps are made to formulate a methodology to „measure“ the risk of fakes.
4. Some Manufacturers improving the fake recognition capability of their products – 2 CC evaluation at BSI
5. Foundation of a technical domain within CC community or ISO for “Security Evaluation of Biometrics”
6. After having a methodology for fingerprint generalizing for other biometrics
Contact

Federal Office for Information Security (BSI)

Axel Munde
Godesberger Allee 185-189
53175 Bonn

Tel: +49 (0)22899-9582-5342
Fax: +49 (0)22899-10-9582-5342

axel.munde@bsi.bund.de
www.bsi.bund.de
www.bsi-fuer-buerger.de