Bundesamt
für Sicherheit in der
Informationstechnik

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

Biometrics and (IT) Security

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

Biometrics and (IT) Security

Challenges of Biometrics

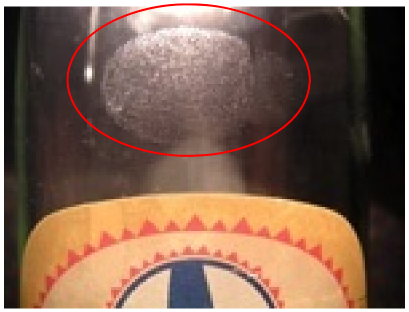
1. FAR / FRR – Statistical properties (BEM <=> SC37 WG5 Standards)
2. Strong and weak biometrics and the “Zoo” (User depending) – Quality related?

   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

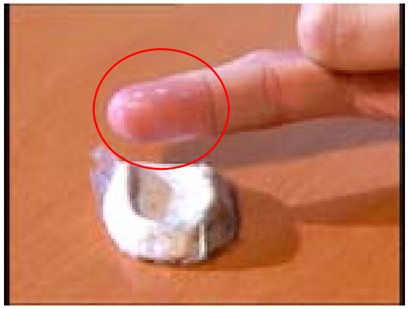


Raw finger image

Digitizing, enhancing and modifying

Printing

wood glue



„Wie können Fingerabdrücke nachgebildet werden? *09. Oktober 2004* (starbug)“
http://dasalte.ccc.de/biometrie/fingerabdruck_kopieren?language=de
http://dasalte.ccc.de/biometrie/fingerabdruck_kopieren?language=en

Faking biometrics - Fingerprints

“ 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)

Mutual recognition symbol

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

Assurance class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Development	ADV_ARC		**1**	1	1	1	1	1
	ADV_FSP	**1**	**2**	**3**	**4**	**5**	5	**6**
	ADV_IMP				**1**	1	**2**	2
	ADV_INT					**2**	**3**	3
	ADV_SPM						**1**	1
	ADV_TDS		**1**	**2**	**3**	**4**	**5**	**6**
Guidance documents	AGD_OPE	**1**	1	1	1	1	1	1
	AGD_PRE	**1**	1	1	1	1	1	1
Life-cycle support	ALC_CMC	**1**	**2**	**3**	**4**	4	**5**	5
	ALC_CMS	**1**	**2**	**3**	**4**	**5**	5	5
	ALC_DEL		**1**	1	1	1	1	1
	ALC_DVS			**1**	1	1	**2**	2
	ALC_FLR							
	ALC_LCD			**1**	1	1	1	**2**
	ALC_TAT				**1**	**2**	**3**	3
Security Target evaluation	ASE_CCL	**1**	1	1	1	1	1	1
	ASE_ECD	**1**	1	1	1	1	1	1
	ASE_INT	**1**	1	1	1	1	1	1
	ASE_OBJ	**1**	**2**	2	2	2	2	2
	ASE_REQ	**1**	**2**	2	2	2	2	2
	ASE_SPD		**1**	1	1	1	1	1
	ASE_TSS	**1**	1	1	1	1	1	1
Tests	ATE_COV		**1**	**2**	2	2	**3**	3
	ATE_DPT			**1**	1	**3**	3	**4**
	ATE_FUN		**1**	1	1	1	**2**	2
	ATE_IND	**1**	**2**	2	2	2	2	**3**
Vulnerability assessment	AVA_VAN	**1**	**2**	2	**3**	**4**	**5**	5

Federal Office
for Information Security

Biometric Protection Profiles – An Overview

1. **Archived U.S. Government Approved Protection Profile - U.S. Government Biometric Verification Mode Protection Profile for Basic Robustness Environments, Version 1.0**
   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

2. **Archived U.S. Government Approved Protection Profile - U.S. Government Biometric Verification Mode Protection Profile for Medium Robustness Environments, Version 1.1**
   http://www.niap-ccevs.org/pp/PP_BVM_MR_V1.1/
   Date: 25 July 2007 – Common Criteria Version: 2.3

   Not assigned to any Validated Products

Biometric Protection Profiles – An Overview

3. **Biometric Device Protection Profile (BDPP)**
   http://www.cesg.gov.uk/policy_technologies/biometrics/media/bdpp082.pdf
   Date: 5. September 2001 – Common Criteria Version: 2.3
   Ever used?

5. **Protection Profile - Biometric Verification Mechanisms Version 1.04**
   (BSI-PP-0016-2005) – Evaluated PP
   https://www.bsi.bund.de/ContentBSI/Themen/ZertifizierungundAnerkennung/ZertifizierungnachCCundITSEC/SchutzprofileProtectionProfile/schutzprofile.html#PP0016
   Date: 17. August 2005 – Common Criteria Version: 2.3
   Based on PP 1. - 3. – Used for 2 Products – 1 under re-evaluation

4. **Biometric Verification Mechanisms Protection Profile Version 1.3**
   (BSI-CC-PP-0043-2008) – Evaluated PP
   https://www.bsi.bund.de/ContentBSI/Themen/ZertifizierungundAnerkennung/ZertifizierungnachCCundITSEC/SchutzprofileProtectionProfile/schutzprofile.html#PP0016
   Date: 07. August 2008 – Common Criteria Version: 3.1 Rev 2

Biometric Protection Profiles – An Overview

6. **Fingerprint Spoof Detection Protection Profile (FSDPP), Version 1.8**
   (BSI-CC-PP-0063-2010)
   https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/ReportePP/pp0063b_pdf.pdf?__blob=publicationFile
   Date: 23th 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)
   https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/ReportePP/pp0062b_pdf.pdf?__blob=publicationFile
   Date: 27th November 2009 – Common Criteria Version: 3.1 Rev 3

How to calculate Attack Potential
- *Elapsed Time* -

Elapsed Time	Factor Value
<= one day	0
<= one week	1
<= two weeks	2
<= one month	4
<= two months	7
<= three months	10
<= four months	13
<= five months	15
<= six months	17
> six months	19

How to calculate Attack Potential
- *Expertise* and *Knowledge of TOE* -

Expertise	Factor Value
Layman	0
Proficient	3(1)
Expert	6
Multiple experts	8
Knowledge of TOE	
Public	0
Restricted	3
Sensitive	7
Critical	11

(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).

Federal Office
for Information Security

How to calculate Attack Potential
- *Window of Opportunity* and *Equipment*-

Window of Opportunity	Factor Value
Unnecessary / unlimited access	0
Easy	1
Moderate	4
Difficult	10
None	(2)

Equipment	Factor Value
Standard	0
Specialised	4(3)
Bespoke	7
Multiple bespoke	9

(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 -

Attack Potential = Elapsed Time + Expertise + Knowledge of TOE + Window of Opportunity + Equipment

Values	Attack potential required to exploit scenario:	TOE resistant to attackers with attack potential of	Meets assurance components	Failure of components
0-9	Basic	No rating	-	AVA_VAN.1 - .5
10-13	Enhanced-Basic	Basic	AVA_VAN.1 - .2	AVA_VAN.3 - .4
14-19	Moderate	Enhanced-Basic	AVA_VAN.1 - .3	AVA_VAN.4 - .5
20-24	High	Moderate	AVA_VAN.1 - .4	AVA_VAN.5
=>25	Beyond High	High	AVA_VAN.1 - .5	

(Fake) Attack Potential
- Examples -

1. Example – Fingerprint System
No fake detection; system commercial available; information in internet, unlimited access

Elapsed Time	<= one week	1
Expertise	Layman	0
Knowledge of TOE	Public	0
Window of Opportunity	Unnecessary / unlimited access	0
Equipment	Standard	0

⇒ Attack potential is 1
⇒ Fails EAL1

(Fake) Attack Potential
- Examples -

2. Example – Fingerprint System
Fake detection; system commercial available; information in internet, limited access (Supervised)

Elapsed Time	<= one week	1
Expertise	Proficient	3
Knowledge of TOE	Public	0
Window of Opportunity	Moderate	4
Equipment	Standard	0

⇒ Attack potential is 8
⇒ Fails EAL1

(Fake) Attack Potential
- Examples -

3. Example – Fingerprint System

Sophisticated fake detection[1]; system not commercial available; information not in internet, limited access (Supervised)

Elapsed Time	<= one month	4
Expertise	Proficient	3
Knowledge of TOE	Restricted	3
Window of Opportunity	Moderate	4
Equipment	Standard	0

⇒ 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

Value	Resistant against attackers with attack potential of:
0 – 4	No rating
5 – 9	**Minimal**
10 – 13	Basic
14 – 19	Enhanced-Basic
20 – 24	Moderate
>= 25	High

Fingerprint Spoof Detection Evaluation Guidance

Testing methodology:

- Main focus: Examination whether spoof detection functionality is able to detect spoofed biometric characteristics with a **sufficient** reliability
- 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