Biometric PAD Toolbox Overview [Toolbox]

Table of Contents

1. Introduction

The TOE may be vulnerable to presentation attacks where attackers attempt to subvert the biometric enrolment or verification by presenting the Presentation Attack Instruments (PAIs). There is a wide range of PAIs that can be used, including natural biometric characteristics, such as dead eyes, or artefacts created from copied or faked characteristics. Using natural biometric characteristics is out of scope of [BIOPP-Module] evaluation and the evaluator shall only use created artefacts to evaluate the TOE.

The toolbox defines the common artefacts for each biometric modality based on publicly available information (e.g. research papers), experiences and knowledge shared among the BIO-iTC members. The evaluator needs to read the [BIOSD] Section 6 as it explains how the evaluator shall use the toolbox during the ATE_IND.1 (Independent testing) and AVA_VAN.1 (Penetration testing) evaluation for PAD in detail.

This overview is originally developed for evaluation activities for FIA_MBV_EXT.3, however, the evaluator can apply the same principles to evaluation activities for FIA_MBE_EXT.3.

2. Biometric modalities supported

Currently toolbox is developed for the following biometric modalities:

- Eye
- Face
  - 2D Image
  - 3D Image
- Fingerprint
- Vein

The toolbox is intended to be a state of the art set of test and is continually updated. The latest versions of the toolbox for each supported modality must be used by the evaluator at the time the testing begins.

3. Purpose of this toolbox overview

This toolbox overview describes common instructions and components for all toolboxes, rather than repeating the same information in each toolbox. The evaluator shall refer both the toolbox overview and the relevant toolbox to perform independent and penetration testing. If there is conflict between the toolbox overview and a toolbox, the toolbox takes precedence over the overview.

4. Structure of the Toolbox

Each toolbox shares the same structure and includes following sections.

***modality name* Toolbox overview**

This section provides specific information only applicable to relevant biometric modality.

***modality name* Toolbox Inventory**

This section categorizes tools and materials that the evaluator shall use to capture a image of biometric characteristics and produce artefacts.

***modality name* Verification List**

This section summarizes all test items that the evaluator shall peform during independent testing. As explained in [BIOSD] Section 6, the evaluator shall select specific test items for penetration testing based on the result of independent testing.

***modality name* References**

This section lists all publicly available information referred to create a toolbox.

Test items

Each test item includes the following sub-sections. This toolbox overview provide a general test protocol in common for all toolboxes and these test items describe more detailed information to

enable repeatable testing.

Sub-section name	Description
Number	Identification number of test
Attack type	Category of attack
Overview	General overview of test
Input	Required input to produce artefacts
Tools	Required tools to capture a image of biometric characteristics and produce artefacts
Recipe	Procedure to create artefacts
Variations	Variants of artefacts to be generated based on this test item. The evaluator shall create those variants by slightly different **Recipe** or with different **Tools** specified here for the independent testing.
Prerequisite	Any conditions that should meet to perform each test
Presentation	Instructions to present artefact to the TOE
Penetration Testing and Attack Potential Rating Suggestions	Suggestions that the evaluator should consider devising penetration tests from this test item and calculate the attack potential rating. The evaluator may change the rating considering actual expertise or knowledge of TOE used to succeed attacks, however, the evaluator shall report such changes with proper justification
Pass Criteria	If this Pass criteria is defined in test items, evaluator shall follow it. Otherwise, the evaluator shall follow criteria defined in this toolbox overview for independent testing and one defined in [BIOSD] Section 9.3 for penetration testing

5. Common guidance for Independent & Vulnerability Testing

As explained in [BIOPP-Module], the TOE is the whole biometric system, including Comparison, Decision and Presentation Attack Detection Subsystems. This means in order to successfully overcome the TOE by the use of artefacts, a genuine person (test subject) has to be enrolled into the TOE, artefacts have to be created referring the toolbox for the corresponding biometric modality and artefacts have to produce a attack presentation match (i.e. a successful presentation attack).

For all types of testing, there are some common steps/procedures to be followed. These are detailed here.

5.1. General test protocol

Presentation attacks can be performed through the following three steps.

5.1.1. Preparation

Before testing can start, the following pre-requisite needs to be met:

- It has to be ensured that the test subject whose body part is used to produce the artefacts for testing is enrolled into the TOE correctly as follows.
  - Enrolment shall be done following guidance provided by the TOE.
  - At least 5 test enrolment transactions shall be performed by the test subject to ensure that the test subject can enrol correctly and be verified after enrolment.
  - In case of repeated failures during the test enrolment, the test subject shall use a different body part (this could mean to use a different finger of the test subject in case of fingerprint verification) and start test enrolment transactions again.
  - If the test subject cannot enrol any body parts during the test enrolment, the test subject shall be exempt from further testing.

5.1.2. Artefact production

Artefact production needs to follow these requirements:

- The evaluator shall document any necessary information so that artefacts used for the test can be re-produced by the evaluator.
- Each produced artefact shall be identified by a unique identifier. This identifier shall be be attached to the artefact at all times (as far as this is possible without destroying the artefact).

5.1.3. Presentation of artefacts

The results of the presentation of artefacts is defined as:

Result	Definition
Successful (Match) Attack	The TOE matches the artefact to the enrolled user
Failed Attack	The TOE rejects the artefact

6. Guidance for Independent Testing (ATE_IND.1)

For independent testing, this guidance is common for all toolboxes. More specific guidance for a specific biometric modality is provided in each toolbox.

This is in addition to guidance in Common guidance for Independent & Vulnerability Testing.

6.1. General test protocol

The presentation attack can be performed through the following two steps after performing Preparation in Section 5.

6.1.1. Artefact production

The production of artefacts for each toolbox shall be performed as follows:

- The evaluator shall produce all artefacts defined in the toolbox.
- The evaluator shall follow instructions in the toolbox to produce artefacts, especially the evaluator shall use tools or materials (e.g. camera, display or printer) that meet requirements in toolbox.
- The evaluator shall produce three artefacts from each test subject.

6.1.2. Presentation of artefacts

The evaluator shall present artefacts to the TOE to perform presentation attacks.

- Each artefact shall be presented to the TOE 10 times

6.2. Number of Subjects

The evaluator shall prepare three test subjects for the above test. A test subject is defined as one individual, and not different body parts from one person (i.e. three fingers from one person could not be considered to be three test subjects for the creation of artefacts).

6.3. Pass/Fail Criteria

The following pass criteria shall be applied if no other criteria are defined in the toolbox.

A TOE passes the test if and only if it reliably defeats the use of **all artefacts (i.e. 3 X 3 = 9 artefacts in total)** that have to be built according to the toolbox. This means that none of the artefacts must be able to reproducibly overcome the TOE.

To reproducibly overcome the TOE by the use of a **certain artefact** in the outlined test scenario is defined as follows:

Table 1. Pass/Fail Criteria

Attempts	**Number of matches**	**Outcome**
10	0	TOE passes this artefact
10	1	TOE passes this artefact
10	2	Additional ten (10) attempts shall be made
20	2	TOE passes this artefact

Attempts	Number of matches	Outcome
Up to 20	3 or more	TOE fails this artefact

The maximum number of attempts allowed with one artefact is twenty (20). If three (3) matches are made to the artefact, the independent test fails (further attempts are not necessary even if 20 total attempts have not yet been made).

7. Guidance for Penetration Testing (AVA_VAN.1)

The evaluator moves to penetration testing only if the TOE passes independent testing. As described in [BIOSD] Section 6, the evaluator shall select those artefacts that show higher imposter attack presentation match rate during independent testing or higher quality artefacts.

This is in addition to guidance in Common guidance for Independent & Vulnerability Testing.

7.1. General test protocol

Presentation attack can be performed through the following two steps after performing Preparation in Section 5.

7.1.1. Artefact production

The production of artefacts for each toolbox shall be performed as follows:

- The evaluator should select artefacts in a toolbox that may produce attack presentation match at higher probability considering the result of independent testing.
- The evaluator may refine the production process of artefacts, as explained in [BIOSD] Section 6. The toolbox describes generalized process to produce artefacts referring to research papers. These research papers may describe more detailed information to produce better artefacts. Such information is valuable if the TOE's PAD algorithm is the same or similar to ones tested by researchers. The evaluator shall consider relevant research papers to be authoritative over the generalized descriptions provided in a toolbox for improving the creation of artefacts.
- The evaluator may produce an arbitrary number of artefacts from each test subject within allowed time period. As described in [BIOSD], both independent and penetration testing shall be finished within one week.

7.1.2. Presentation of artefacts

The evaluator shall present artefacts to the TOE to perform presentation attacks.

- Each artefact shall be presented to the TOE an arbitrary number of times within allowed time period. As described in [BIOSD], both independent and penetration testing shall be finished within one week.

7.2. Number of Subjects

If the evaluator can create artefacts that produce an attack presentation match during independent testing, the evaluator should select the test subjects whose artefacts had successful matches and increase the number of attempts. The evaluator may replace the test subject for penetration testing as described in [BIOSD] Section 6.

7.3. Pass/Fail Criteria

As described in [BIOSD], both independent and penetration testing shall be finished within one week. The evaluator may select one or two artefacts and perform an arbitrary number of attempts within this time period. If the evaluator can create artefacts that meet the criteria defined in [BIOSD] Section 9.3, the TOE fails AVA_VAN.1 evaluation.

8. Related Documents

- [BIOPP-Module] collaborative PP-Module for Biometric enrolment and verification - for unlocking the device -, March 13, 2020, Version 0.95
- [BIOSD] Supporting Document Mandatory Technical Document: Evaluation Activities for collaborative PP-Module for Biometric enrolment and verification - for unlocking the device -, March 13, 2020, Version 0.95

9. Revision History

Table 2. Revision history

Version	Date	Description
0.3	May 30, 2019	Public Review Draft 1
0.5	December 20, 2019	Public Review Draft 2
0.6	March 13, 2020	Proposed Release