INTERNATIONAL STANDARD

ISO/IEC 30107-3

First edition
2017-09

Information technology — Biometric presentation attack detection —

Part 3: Testing and reporting

Technologies de l'information — Détection d'attaque de présentation en biométrie —

Partie 3: Essais et rapports d'essai

IECNORM.COM : Click to view the full PDF of ISO/IEC 30107-3:2017

Reference number
ISO/IEC 30107-3:2017(E)

© ISO/IEC 2017

IECNORM.COM : Click to view the full PDF of ISO/IEC 30107-3:2017

COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2017, Published in Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

 © ISO/IEC 2017 – All rights reserved

Contents

Page

IECNORM.COM : Click to view the full PDF of ISO/IEC 30107-3:2017

© ISO/IEC 2017 – All rights reserved

IECNORM.COM : Click to view the full PDF of ISO/IEC 30107-3:2017

© ISO/IEC 2017 – All rights reserved

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see the following URL: www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/IEC JTC 1, *Information technology*, SC 37, *Biometrics*.

A list of all parts in the ISO 30107 series can be found on the ISO website.

IECNORM.COM : Click to view the full PDF of ISO/IEC 30107-3:2017

© ISO/IEC 2017 – All rights reserved

Introduction

The presentation of an artefact or of human characteristics to a biometric capture subsystem in a fashion intended to interfere with system policy is referred to as a presentation attack. ISO/IEC 30107 (all parts) addresses techniques for the automated detection of presentation attacks. These techniques are called presentation attack detection (PAD) mechanisms.

As is the case for biometric recognition, PAD mechanisms are subject to false positive and false negative errors. False positive errors wrongly categorize bona fide presentations as attack presentations, potentially flagging or inconveniencing legitimate users. False negative errors wrongly categorize presentation attacks (also known as attack presentations) as bona fide presentations, potentially resulting in a security breach.

Therefore, the decision to use a specific implementation of PAD will depend upon the requirements of the application and consideration of the trade-offs with respect to security, evidence strength, and efficiency.

The purpose of this document is as follows:

— to define terms related to biometric presentation attack detection testing and reporting, and

— to specify principles and methods of performance assessment of biometric presentation attack detection, including metrics.

This document is directed at vendors or test labs seeking to conduct evaluations of PAD mechanisms.

Biometric performance testing terminology, practices, and methodologies for statistical analysis have been standardized through ISO and Common Criteria. Metrics such as FAR, FRR, and FTE are widely used to characterize biometric system performance. Biometric performance testing terminology, practices, and methodologies for statistical analysis are only partially applicable to the evaluation of PAD mechanisms due to significant, fundamental differences between biometric performance testing concepts and PAD mechanism testing concepts. These differences can be categorized as follows:

a) **Statistical significance**

Biometric performance testing utilizes a statistically significant number of test subjects representative of the targeted user group. Error rates are not expected to vary significantly when adding more test subjects or using a completely different group. Generally, taking more measurements increases the accuracy of the error rates.

In PAD testing, many biometric modalities can be attacked by a large or indeterminate number of potential presentation attack instrument (PAI) species. In these cases, it is very difficult or even impossible to have a comprehensive model of all possible presentation attack instruments. Hence, it could be impossible to find a representative set of PAI species for the evaluation. Therefore, measured error rates of one set of presentation attack instruments cannot be assumed to be applicable to a different set.

PAI species present a source of systematic variation in a test. Different PAI may have significantly different error rates. Additionally, within any given PAI species, there will be random variation across instances of the PAI series. The number of presentations required for a statistically significant test will scale linearly with the number of PAI species of interest. Within each PAI species, the uncertainty associated with a PAD error rate estimate will depend on the number of artefacts tested and the number of individuals.

EXAMPLE 1 In fingerprint biometrics, many potent artefact materials are known, but any material or material mixture that can present fingerprint features to a biometric sensor is a possible candidate. Since artefact properties such as age, thickness, moisture, temperature, mixture rates, and manufacturing practices can have a significant influence on the output of the PAD mechanism, it is easy to define tens of thousands of PAI species using current materials. Hundreds of thousands of presentations would be needed for a proper statistical analysis – even then, resulting error rates could not be transferred to the next set of new materials.

IECNORM.COM : Click to view the full PDF of ISO/IEC 30107-3:2017

 © ISO/IEC 2017 – All rights reserved

b) **Comparability of test results across systems**

In biometric performance testing, application-specific error rates based on the same corpus of biometric samples can be used to compare different biometric systems or different configurations. The meaning of "better" and "worse" is generally understood.

By contrast, when using error rates to benchmark PAD mechanisms, terms such as "better" can be highly dependent on the intended application.

EXAMPLE 2 In a given testing scenario with 10 PAI species (presented 100 times), $System_1$ detects 90 % of attack presentations and $System_2$ detects 85 %. $System_1$ detects all presentations for 9 PAI species but fails to detect all presentations with the 10th PAI species. $System_2$ detects 85 % of all PAI species. Which is better? In a security analysis, $System_1$ would be worse than $System_2$, because revealing the 10th PAI species would orient an attacker such that he could use this method to defeat the capture device all the time. However, if attackers could be prevented from using the 10th PAI species, $System_1$ would be better than $System_2$, because individual rates indicate that it is possible to overcome $System_2$ with all PAI species.

c) **Cooperation**

Many biometric performance tests address applications such as access control in which subjects are cooperative. Errors due to incorrect operation are an issue of a lack of knowledge, experience or guidance rather than intent. Significant uncooperative behaviour in a group is not part of the underlying "biometric model" and would render the determined error rates almost useless for biometric performance testing.

PAD tests include subjects whose behaviour is not cooperative. Attackers will try to find and exploit any weakness of the biometric system, circumventing or manipulating its intended operation. Presentation attack types, based on the experience and knowledge of the tester, can change the success rates for an attack dramatically. Hence, it can be difficult to define testing procedures that measure error rates in a fashion representative of cooperative behaviour.

d) **Automated testing**

In biometric performance testing, it is often possible to test comparison algorithms using databases from devices or sensors of similar quality. Performance can be measured in a technology evaluation using previously collected corpuses of samples as specified in ISO/IEC 19795-1.

In PAD testing, data from the biometric sensor (e.g. digitized fingerprint images) may be insufficient to conduct evaluations. Biometric systems with PAD mechanisms often contain additional sensors to detect specific properties of a biometric characteristic. Hence, a database previously collected for a specific biometric system or configuration may not be suitable for another biometric system or configuration. Even slight changes in the hardware or software could make earlier measurements useless. It is generally impractical to store multivariate synchronized PAD signals and replay them in automated testing. Therefore, automated testing is often not an option for testing and evaluating PAD mechanisms.

e) **Quality and performance**

In biometric performance testing, performance is usually linked directly to biometric data quality. Low-quality samples generally result in higher error rates while a test with only high-quality samples will generally result in lower error rates. Hence, quality metrics are often used to improve performance (dependent on the application).

In PAD testing, even though low biometric quality can cause an artefact to be unsuccessful, there is no reason to assume a certain quality level from artefacts in general. Samples from artefacts can exhibit better quality than samples from human biometric characteristics. Absent a model of attacker skill, it seems valid (at least in a security evaluation) to assume a "worst case" scenario where the attacker always uses the best possible quality. That way, one can at least determine a guaranteed minimal detection rate for the specific test set while reducing the number of necessary tests at the same time. It is then a matter of rating the attack potential of successful artefacts (effort and expertise for the needed quality) in order to assess the security level, as is the practice in Common Criteria evaluations.

IECNORM.COM : Click to view the full PDF of ISO/IEC 30107-3:2017

© ISO/IEC 2017 – All rights reserved

Based on the differences a) through e), the following general comments regarding error rates and metrics related to PAD mechanisms can be derived:

— In an evaluation, PAI species are analysed/rated separately.

— Attack presentation classification error rates other than 0 % for a PAI species only prove that the PAI can be successful. A different tester might achieve a higher or lower attack presentation classification error rate. Further, training to identify the relevant material and presentation parameters could increase the attack presentation classification error rate for this PAI species. The experience and knowledge of the tester, as well as the availability of the necessary resources, are significant factors in PAD testing and are taken into account when conducting comparisons or performance analysis.

— Error rates for PAD mechanisms are determined by the specific context of the given PAD mechanism, the set of PAI species, the application, the test approach, and the tester. Error rates for PAD mechanisms are not necessarily comparable across similar tests, and error rates for PAD mechanisms are not necessarily reproducible by different test laboratories.

IECNORM.COM : Click to view the full PDF of ISO/IEC 30107-3:2017

© ISO/IEC 2017 – All rights reserved

Information technology — Biometric presentation attack detection —

Part 3: Testing and reporting

IECNORM.COM : Click to view the full PDF of ISO/IEC 30107-3:2017

1 Scope

This document establishes:

— principles and methods for performance assessment of presentation attack detection mechanisms;

— reporting of testing results from evaluations of presentation attack detection mechanisms;

— a classification of known attack types (in an informative annex).

Outside the scope are:

— standardization of specific PAD mechanisms;

— detailed information about countermeasures (i.e. anti-spoofing techniques), algorithms, or sensors;

— overall system-level security or vulnerability assessment.

The attacks considered in this document take place at the sensor during presentation. Any other attacks are considered outside the scope of this document.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 2382-37, *Information technology — Vocabulary — Part 37: Biometrics*

ISO/IEC 19795-1:2006, *Information technology — Biometric performance testing and reporting — Part 1: Principles and framework*

ISO/IEC 30107-1:2016, *Information technology — Biometric presentation attack detection — Part 1: Framework*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 2382-37 and ISO/IEC 30107-1 and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— IEC Electropedia: available at http://www.electropedia.org/

— ISO Online browsing platform: available at http://www.iso.org/obp

© ISO/IEC 2017 – All rights reserved

3.1 Attack elements

3.1.1
presentation attack
attack presentation
presentation to the biometric data capture subsystem with the goal of interfering with the operation of the biometric system

Note 1 to entry: An attack presentation might be a single attempt, a multi-attempt transaction, or some other type of interaction with a subsystem.

3.1.2
bona fide presentation
interaction of the biometric capture subject and the biometric data capture subsystem in the fashion intended by the policy of the biometric system

Note 1 to entry: Bona fide is analogous to normal or routine, when referring to a bona fide presentation.

Note 2 to entry: Bona fide presentations can include those in which the user has a low level of training or skill. Bona fide presentations encompass the totality of good-faith presentations to a biometric data capture subsystem.

3.1.3
attack type
element and characteristic of a presentation attack, including PAI species, concealer or impostor attack, degree of supervision, and method of interaction with the capture device

3.1.4
test approach
totality of considerations and factors involved in PAD evaluation

Note 1 to entry: Elements of a test approach are given in Clauses 7 to 11.

Note 2 to entry: A test approach refers to all processes, factors, and aspects specified in the course of the evaluation.

3.1.5
item under test
IUT
implementation that is the object of a test assertion or test case

Note 1 to entry: The IUT is the equivalent of TOE in Common Criteria evaluations.

3.1.6
PAI species
class of presentation attack instruments created using a common production method and based on different biometric characteristics

EXAMPLE 1 A set of fake fingerprints all made in the same way with the same materials but with different friction ridge patterns would constitute a PAI species.

EXAMPLE 2 A specific type of alteration made to the fingerprints of several data capture subjects would constitute a PAI species.

Note 1 to entry: The term “recipe” is often used to refer to how to make a PAI species.

Note 2 to entry: Presentation attack instruments of the same species may have different success rates due to variability in the production process.

IECNORM.COM : Click to view the full PDF of ISO/IEC 30107-3:2017

© ISO/IEC 2017 – All rights reserved

3.1.7
PAI series
presentation attack instruments based on a common medium and production method and a single biometric characteristic source

EXAMPLE A set of fake fingerprints all made in the same way with the same materials and with the same friction ridge pattern.

Note 1 to entry: Depending on the experimental goals, an evaluation may utilize series from one source or from several. While tests involving several biometric sources may demonstrate generality of a PAI species, they add variation associated with individual human traits.

3.1.8
target of evaluation
TOE
within Common Criteria, the IT product that is the subject of the evaluation

Note 1 to entry: The TOE is the equivalent of IUT in Common Criteria evaluations.

3.1.9
attack potential
measure of the capability to attack a TOE given the attacker's knowledge, proficiency, resources and motivation

3.2 Metrics

3.2.1
attack presentation classification error rate
APCER
proportion of attack presentations using the same PAI species incorrectly classified as bona fide presentations in a specific scenario

3.2.2
bona fide presentation classification error rate
BPCER
proportion of bona fide presentations incorrectly classified as presentation attacks in a specific scenario

3.2.3
attack presentation non-response rate
APNRR
proportion of attack presentations using the same PAI species that cause no response at the PAD subsystem or data capture subsystem

EXAMPLE A fingerprint system may not register or react to the presentation of a PAI due to the PAI's lack of realism.

3.2.4
bona fide presentation non-response rate
BPNRR
proportion of bona fide presentations that cause no response at the PAD subsystem or data capture subsystem

3.2.5
attack presentation acquisition rate
APAR
proportion of attack presentations using the same PAI species from which the data capture subsystem acquires a biometric sample of sufficient quality

IECNORM.COM : Click to view the full PDF of ISO/IEC 30107-3:2017

© ISO/IEC 2017 – All rights reserved

3.2.6
impostor attack presentation match rate
IAPMR
<full-system evaluation of a verification system> proportion of impostor attack presentations using the same PAI species in which the target reference is matched

3.2.7
concealer attack presentation non-match rate
CAPNMR
<full-system evaluation of a verification system> proportion of concealer attack presentations using the same PAI species in which the reference of the concealer is not matched

3.2.8
impostor attack presentation identification rate
IAPIR
<full-system evaluation of an identification system> proportion of impostor attack presentations using the same PAI species in which the targeted reference identifier is among the identifiers returned or, depending on intended use case, at least one identifier is returned by the system

Note 1 to entry: An attacker might be both an impostor (trying to match an existing non-self enrolee) and a concealer (obscuring his real biometric sample with a PAI).

3.2.9
concealer attack presentation non-identification rate
CAPNIR
<full-system evaluation of an identification system> proportion of concealer presentation attacks using the same PAI species in which the reference identifier of the concealer is not among the identifiers returned or, depending on intended use case, in which no identifiers are returned

Note 1 to entry: In a negative identification system, such as a black-list, the concealer could intend that no identifiers are returned to avoid scrutiny by a human operator.

3.2.10
PAD subsystem processing duration
PS-PD
duration required for the PAD subsystem to classify PAD data

3.2.11
data capture subsystem processing duration
DCS-PD
duration required for the data capture subsystem to acquire a sample, inclusive of PAD subsystem processing duration (if applicable)

3.2.12
full-system processing duration
FS-PD
duration required for the data capture subsystem and comparison subsystem to acquire and process a sample, inclusive of PAD subsystem processing duration (if applicable)

IECNORM.COM : Click to view the full PDF of ISO/IEC 30107-3:2017

4 Abbreviated terms

The abbreviated terms shown in Table 1 are used in this document.

Table 1 — Abbreviated terms

APCER	Attack Presentation Classification Error Rate
APAR	Attack Presentation Acquisition Rate
APNRR	Attack Presentation Non-Response Rate

© ISO/IEC 2017 – All rights reserved

Table 1 *(continued)*

BPCER	Bona Fide Presentation Classification Error Rate
BPNRR	Bona Fide Presentation Non-Response Rate
CCRA	Common Criteria Recognition Arrangement
CAPNIR	Concealer Attack Presentation Non-Identification Rate
CAPNMR	Concealer Attack Presentation Non-Match Rate
DCS-PD	Data Capture Subsystem Processing Duration
EAL	Evaluation Assurance Level
FTA	Failure to Acquire Rate
FTE	Failure to Enrol Rate
FAR	False Accept Rate
FNIR	False Negative Identification Rate
FPIR	False Positive Identification Rate
FRR	False Reject Rate
FSDPP	Fingerprint Spoof Detection Protection Profiles
FS-PD	Full-System Processing Duration
IAPIR	Impostor Attack Presentation Identification Rate
IAPMR	Impostor Attack Presentation Match Rate
IUT	Item Under Test
PS-PD	PAD Subsystem Processing Duration
PAD	Presentation Attack Detection
PAI	Presentation Attack Instrument
PAIS	Presentation Attack Instrument Species
TOE	Target of Evaluation

IECNORM.COM : Click to view the full PDF of ISO/IEC 30107-3:2017

5 Conformance

To conform to this document, an evaluation of PAD mechanisms shall be planned, executed and reported in accordance with the mandatory requirements as follows:

— Clause 6 to 11.1;

— Clause 13.1;

— for evaluations of PAD mechanisms in enrolment, see 11.2;

— for evaluations of PAD mechanisms in verification, see 11.3;

— for evaluations of PAD mechanisms in positive or negative identification, see 11.4;

— for PAD subsystem evaluations, see 13.2;

— for data capture subsystem evaluations, see 13.3;

— for full-system evaluations of verification systems, see 13.4.2.1;

— for full-system evaluations of positive identification systems, see 13.4.2.2;

— for full-system evaluations of negative identification systems, see 13.4.2.3.

© ISO/IEC 2017 – All rights reserved

6 Presentation attack detection overview

This document describes two types of presentation attackers: biometric impostors (a.k.a. impersonators) and biometric concealers. These types of attackers differ in that biometric impostors typically need to defeat PAD subsystems, pass quality checks, and match through comparison subsystems, whereas biometric concealers do not need to match through comparison subsystems.

While the desired impersonation or concealment outcome may lend itself towards a sub-set of attack types, any type of PAI can be used by either type of attacker.

Evaluations of PAD mechanisms and resulting reports shall specify the type of presentation attacker, biometric impostor or biometric concealer, considered in an evaluation.

Evaluations of PAD mechanisms are classifiable as one of three general types, increasing in specificity, as follows:

— generic, broad evaluations of PAD mechanisms of any device for an unknown application;

— application-focused evaluations of PAD mechanisms in which the set/range of attack types is selected to be appropriate to the application, such as those discussed in Clause 11;

— product-specific evaluations of PAD mechanisms, used to test a supplier's claim of performance against a specific category of attack types.

Evaluations of PAD mechanisms and resulting reports shall describe the type of evaluation conducted as well as the attack types to be tested.

7 Levels of evaluation of PAD mechanisms

7.1 Overview

Evaluation of PAD mechanisms is determined by the item under test (IUT). PAD evaluations and resulting reports shall fully describe the IUT, including all configurations and settings as well as the amount of information available to the evaluator about PAD mechanisms in place. IUTs shall be categorized as follows:

— PAD subsystem;

— data capture subsystem;

— full system.

A **PAD subsystem** is a hardware and/or software that implements a PAD mechanism and makes an explicit declaration regarding the detection of presentation attacks. Results of the PAD mechanism are accessible to the evaluator and are an aspect of the evaluation.

EXAMPLE 1 A PAD subsystem could be a fingerprint device that logs a PAD score or decision when a PAI is presented.

A **data capture subsystem**, consisting of capture hardware or/and software, couples PAD mechanisms and quality checks in a fashion opaque to the evaluator. The evaluator may not necessarily know whether the data capture subsystem utilizes presentation attack detection. Acquisition may be for the purpose of enrolment or recognition, but no comparison takes place in the data capture subsystem.

EXAMPLE 2 A data capture subsystem could be an iris collection device that fails to acquire a sample from an iris artefact, where it is impossible to determine whether failure to acquire is due to a liveness check or quality check (the implementation does not provide this level of transparency).

NOTE For simplicity, the term "quality check" encompasses feature extraction, segmentation, or any other automated processing function used to validate the utility of a biometric sample.

IECNORM.COM : Click to view the full PDF of ISO/IEC 30107-3:2017

 © ISO/IEC 2017 – All rights reserved

A **full system** adds biometric comparison to the PAD subsystem or data capture subsystem, comprising a full end-to-end system. This leads to additional failure points for the PAI beyond PAD mechanisms and quality checks. In a full system, there might be one or multiple PAD mechanisms at different points in the system.

Evaluations of PAD mechanisms and resulting reports shall specify the applicable evaluation level, whether PAD subsystem, data capture subsystem, or full system. The resulting reports should discuss how the evaluation level influenced PAD testing.

7.2 General principles of evaluation of PAD mechanisms

Evaluations of PAD mechanisms shall cover a defined variety of attack types by utilizing a representative set of presentation attack instruments and a representative set of bona fide capture subjects.

For the set of presentation attack instruments, evaluations of PAD mechanisms should be based on the appropriate evaluation type (see Clause 6) and on relevant attack types. Not all PAD mechanisms are designed to address all possible presentation attacks.

EXAMPLE A PAD mechanism designed to recognize an artificial biometric characteristic is not likely to be effective for detecting an altered biometric characteristic.

Once the types are defined, the number and range of presentation attack instruments to be evaluated should be specified. Establishing whether a specific attack type reproducibly succeeds does not require a very large number of presentations.

The evaluator shall define the parameters of the attack presentation to fully characterize the range of attacker interactions with the IUT, to include the temporal boundaries of the presentation.

A representative set of bona fide capture subjects is required to determine the frequency with which the PAD mechanism incorrectly classifies bona fide presentations. This is a critical part of PAD testing since a PAD mechanism could erroneously classify bona fide presentations as attack presentations. A high classification error rate for bona fide capture subjects would reduce system usability.

The representativeness of bona fide presentations should consider test subject selection and size as described in ISO/IEC 19795-1:2006, 6.5 and 6.6. Particularly, total numbers of bona fide presentations should exceed that required by Rule of 30.

In an evaluation of PAD mechanisms, the evaluator shall (1) define bona fide presentations and representative capture subjects for the target application and population and (2) provide a rationale for these definitions.

NOTE Defining "bona fide" presentations and representative capture subjects can be a challenge in evaluations of PAD mechanisms. In some cases, the evaluator may define bona fide presentations as those that conform to vendor or implementer specifications. However, in certain applications, bona fide or representative capture subject interaction with data capture devices may encompass a wide range of behaviours and conditions. For example, a vendor may define a conformant presentation to a fingerprint sensor as one conducted with clean fingerprints. While one could conduct a test in which all capture subjects without perfectly clean fingerprints are excluded, it is reasonable to expect that operational systems have some tolerance for a range of regular, reasonable, or typical fingerprint conditions. Otherwise, operational systems would have excessively high false rejection or failure to enrol (FTE) rates. This is particularly relevant to PAD testing, because bona fide presentation classification errors may be most frequently encountered among data capture subjects whose interactions with data capture devices, while sufficient for enrolment or biometric recognition, are only marginally conformant with vendor specifications.

7.3 PAD subsystem evaluation

PAD subsystem evaluations measure the ability of the PAD subsystem to correctly classify both attack presentations and bona fide presentations. An effective attack presentation will be incorrectly classified as a bona fide presentation, resulting in the defeat of the PAD subsystem.

IECNORM.COM : Click to view the full PDF of ISO/IEC 30107-3:2017

© ISO/IEC 2017 – All rights reserved

PAD subsystem evaluations may focus on the effectiveness of the sensor (mostly hardware or possibly internal firmware) in terms of refusal to acquire a sample, including cases with or without automated indications of refusal. Such evaluations focus on rejecting presentation attack instruments. The output of the PAD subsystem could be discrete, such as a pass/fail to each PAI utilized.

Alternatively, PAD subsystem evaluations may focus on the effectiveness of a PAD algorithm (exemplified by LivDet[8]). This type of PAD subsystem evaluation can be performed offline with a corpus of samples; the PAD subsystem determines whether samples come from an attack. Such tests are typically based on a collected database, analogous to technology tests in biometric performance evaluations.

If the PAD subsystem returns a PAD score, false-negative and false-positive error rates can be expressed parametrically as functions of the decision threshold (e.g. through a detection error trade-off curve).

Clause 10 provides an overview of factors that need to be considered when designing a test for PAD subsystems designed to recognize artefacts.

7.4 Data capture subsystem evaluation

In data capture subsystems, presentation attacks may fail for reasons other than detection in the PAD subsystem. For example, the data capture subsystem may fail to respond to a presentation attack, or a quality subsystem may reject the presentation attack. In data capture subsystems where PAD mechanisms are not implemented or where the evaluator does not have access to results of PAD mechanisms, outcomes are based on whether the data capture subsystem has successfully acquired a sample. An effective presentation attack will defeat both the PAD subsystem (if present and active) and the quality subsystem, resulting in the capture of a biometric sample.

7.5 Full-system evaluation

Full-system evaluations add a comparison subsystem to the IUT, generating a comparison score or candidate list. This is illustrated in ISO/IEC 30107-1:2016, Figure 3.

Depending on the implementation, a full-system evaluation may encompass:

— **PAD subsystem, data capture subsystem, and comparison subsystem** (for IUTs in which results of the PAD mechanism are accessible to the evaluator). In this type of evaluation, testing corresponds to a scenario test with known attackers within the test crew. Presentation attacks are intended to subvert the PAD subsystem, data capture subsystem, and comparison subsystem. A successful presentation attack will defeat both the PAD subsystem and the data capture subsystem, resulting in the capture of a biometric sample. Subsequently, the biometric sample will be submitted for processing by the comparison subsystem.

— **Data capture subsystem and comparison subsystem** (for IUTs in which PAD results are not accessible to the evaluator). In this type of evaluation, testing corresponds to a scenario test with known attackers within the test crew. Presentation attacks are intended to subvert the data capture subsystem and comparison subsystem. A successful presentation attack will defeat the data capture subsystem, resulting in the capture of a biometric sample. Subsequently, the biometric sample will be submitted for processing by the comparison subsystem.

— **PAD subsystem and comparison subsystem** (for IUTs in which a corpus of samples is evaluated in an offline mode). In this type of evaluation, testing corresponds to a technology test with samples from presentation attacks in the corpus.

— **Comparison subsystem** (for IUTs in which comparator results and PAD mechanism results are indistinguishable).

IECNORM.COM : Click to view the full PDF of ISO/IEC 30107-3:2017

© ISO/IEC 2017 – All rights reserved

The objective of the attacker becomes critical in full-system evaluations because the outcome of the comparison subsystem dictates whether an attack was successful. Considerations are as follows:

— **Verification systems.** In the case of an impostor/access seeker attack, failure to match (i.e. rejection of the PAI by the comparator) is typically considered a successful outcome from the perspective of the system designer.

— **Positive identification systems.** In the case of an impostor/access seeker attack, failure to return a targeted identifier (i.e. the comparator does not match the PAI against a targeted enrolment) is typically considered a successful outcome from the perspective of the system designer.

— **Negative identification systems.** In the case of an identity concealer, returning an identifier associated with the concealed identity (i.e. the comparator matches the concealed characteristic against its enrolment) is typically considered a successful outcome from the perspective of the system designer.

NOTE In a black-list system, if any returned identifier triggers an investigation that uncovers the attack, this is typically considered a successful outcome from the perspective of the system designer.

8 Artefact properties

8.1 Properties of presentation attack instruments in biometric impostor attacks

In biometric impostor attacks, the attacker intends to be recognized as an individual other than him/herself.

For biometric impostor attacks in which the subject intends to be recognized as a specific, targeted individual known to the system, it will be necessary to create an artefact with three properties:

— Property 1. The sample appears as a natural biometric characteristic to any PAD mechanisms in place.

— Property 2. The sample appears as a natural biometric characteristic to any biometric data quality checks in place.

— Property 3. A sample acquired by a capture device from the artefact contains extractable features that match against the targeted individual's reference.

With regard to Property 1, an evaluator may or may not have information on the PAD mechanisms in place for a given system. Understanding the PAD mechanisms implemented is likely to motivate the use of materials capable of appearing as natural biometric characteristics.

Property 3 is related to the signal processing and comparison mechanisms within the biometric system and is not generally considered a part of the PAD mechanism.

NOTE 1 These issues have been discussed in References [19] to [21] and may require the use of new materials.

EXAMPLE Animal proteins[21] can be used to defeat PADs found in fingerprint systems such as in Reference [18]. If the sample does not appear as natural to the PAD, the sample can be treated temporarily to affect such an appearance[20].

The most straightforward way to affect Property 3 is to create a copy of the targeted individual's biometric characteristic. In some cases, it is possible to produce a copy of a physical biometric characteristic in the form of an artificial biometric characteristic which can be used for a presentation attack. Alternatively, if a copy of the targeted individual's enrolled reference can be obtained, an attacker may be able to create an artefact capable of being acquired by the sensor to produce a signal matchable to that reference. Such artefacts may be required to pass biometric sample quality checks.

Regarding attacks by a biometric impostor, attackers may acquire a capture subject's biometric characteristic directly from the capture subject. Such acquisition may be cooperative (e.g. the capture subject provides a fingerprint to a sensor) or non-cooperative (e.g. the capture subject leaves a fingerprint on a glass or a biometric capture device allowing the attacker to lift the fingerprint).

IECNORM.COM : Click to view the full PDF of ISO/IEC 30107-3:2017

© ISO/IEC 2017 – All rights reserved

Additionally, faces or voices can be recorded by attackers with a camera or microphone. Different attack scenarios are associated with cooperative and non- cooperative characteristic data capture. Artefacts created from cooperative acquisitions may be of higher quality than those from non-cooperative acquisition, which may in turn impact PAD rates and biometric performance rates.

NOTE 2 A subject can be coerced to submit high-quality samples, in which case the cooperative/non-cooperative distinction is not applicable.

For biometric impostor attacks in which the subject intends to be recognized as any individual already known to the system, without regard to which individual, a sample acquired by a sensor from the artefact should have characteristics that can match one or more stored references when processed. The most straightforward way to affect Property 3 is to have knowledge of some of the references stored in the system. Absent such knowledge, it is possible to experiment against similar biometric systems using characteristics from the enrolled population or a general population model as a proxy. Such experiments may provide insight into the probability of successful identification against one or more enrolled references.

Artefacts aiming at arbitrary subject impersonation may be referred to as "wolf artefacts". Artefacts used by data capture subjects during enrolment intended to achieve high impostor attack presentation match rate (IAPMR) may be referred to as "lamb artefacts".

If the biometric impostor intends to utilize the disguised or altered biometric characteristic multiple times, then multiple copies of the PAI should be manufacturable, or a single PAI should have a life-span sufficient for the duration of the intended use. This may impact the choice of material or production method.

8.2 Properties of presentation attack instruments in biometric concealer attacks

In the biometric concealer attack, the attacker seeks to conceal his/her own biometric characteristics, either using an artefact or through disguise or alteration of natural biometric characteristics.

Artefacts created for the biometric concealer attack are meant to appear as a natural biometric characteristic to any PAD mechanisms and any biometric quality checks in place. Such artefacts should contain extractable features that can be compared to stored references. In addition to Properties 1 and 2, artefacts in biometric concealer attacks should also have the following property (continuing the list of properties from 8.1):

— Property 4. The extractable features should not match any stored references.

Property 4 is related to the signal processing and comparison mechanisms within the biometric system and is not part of the PAD mechanism.

Artefacts unable to generate features capable of further processing by the biometric system may trigger a "failure to acquire" signal within the system, leading to additional sample acquisition attempts or triggering an "exception handling" process. Both of these outcomes are undesirable by the attacker.

NOTE 1 Poorly designed biometric systems have been known to generate "null" feature sets (feature sets containing no information), which then can be successfully compared to a similar "null" reference (sample, features, or models containing no information). Consequently, the necessity of compliance with Property 4 for a successful attack will depend upon the sophistication of the biometric system.

NOTE 2 Artefacts aiming at achieving high failure to acquire (FTA) or concealer attack presentation non-match rate (CAPNMR) can be referred to as "goat artefacts".

In an identification system, compliance with Property 4 is a function of the number of stored references and the identification thresholds and policies in place.

8.3 Properties of synthesized biometric samples with abnormal characteristics

If a biometric system produces unusually high false match rates when presented with certain abnormal biometric characteristics, this may warrant specific evaluation techniques. Examples of abnormal characteristics could include those with unusually large or small numbers of features.

IECNORM.COM : Click to view the full PDF of ISO/IEC 30107-3:2017

 © ISO/IEC 2017 – All rights reserved

Such characteristics may not be representative of any human biometric characteristic but could be synthesized and copied to an artefact. Such a characteristic might match against a wide range of enrolees. An evaluation may seek to determine whether synthesized biometric characteristics with abnormal properties are accepted by the biometric system and can result in higher-than-normal IAPMR against bona fide enrolee references.

Evaluations of PAD mechanisms and resulting reports that examine the efficacy of synthesized biometrics samples with abnormal properties shall detail (1) findings for acceptance of synthesized biometric samples with abnormal properties and (2) the degree of impact on IAPMR when using synthesized biometric samples with abnormal properties.

9 Considerations in non-conformant capture attempts of biometric characteristics

9.1 Methods of presentation

Capture subjects may intentionally change their biometric characteristics or the presentation of the characteristics in an attempt to avoid recognition or to impersonate an enrolee. For biometric modes such as voice and dynamic signature, capture subjects can intentionally modify their behaviours. For biometric modes such as fingerprint, a capture subject could intentionally manipulate the presentation of their characteristic to the capture device in order to produce a non-conformant captured sample. When the capture subject behaves in this way, the presentation shall be considered an attack, not a bona fide presentation, and the capture subject shall be denominated as an attacker.

Artefact detection techniques are not designed to detect non-conformant bona fide presentations.

9.2 Methods of assessment

All biometric characteristics are susceptible to capture subject-induced changes caused by capture subject behaviours. To determine the sensitivity of error rates to deliberate, capture subject-induced changes in biometric characteristics or presentation, evaluators can conduct a representative test of such changes' effect on error rates such as FTA and false non-match rate. If evaluation resources and time allow, sufficient trials may also be run to determine the effect on false match rate.

10 Artefact creation and usage in evaluations of PAD mechanisms

10.1 General

Evaluations of PAD mechanisms may be designed to answer the following questions:

— How consistently does a specific artefact subvert a biometric system?

— What factors influence the efficacy of artefact-based biometric system attack?

— What attack types with the lowest attack potential succeed in subverting the biometric system?

Artefact creation, provenance, usage, and handling – from creation to utilization – are central to evaluation of PAD mechanisms.

IECNORM.COM : Click to view the full PDF of ISO/IEC 30107-3:2017

© ISO/IEC 2017 – All rights reserved

10.2 Artefact creation and preparation

In an evaluation of PAD mechanisms, one or more PAI species will be selected. When creating and preparing artefacts according to a selected PAI species, the following factors and parameters should be considered:

— Artefact creation process: artefact creation (or fabrication) may be based on multiple materials whose production, treatment, and handling can impact artefact efficacy. Artefacts are not necessarily machine-generated finished products, and human factors can impact artefact performance.

— Artefact preparation process: artefacts may require treatment or preparation between creation and utilization.

— Effort required to create and prepare artefacts: for example, skills required, technical know-how, creation time, difficulty of procuring material and equipment to be used.

— Artefact creation consistency: a "production run" of artefacts, whether comprised of several artefacts created in succession or created over a long span of time, may result in artefact-over-artefact efficacy variations. This may be due to variation in materials composition, handling anomalies, or environmental factors.

— Artefact customization for a specific capture subject: a given artefact may only be suited for use by a specific capture subject for whom it has been custom-designed, or whose biometric characteristics are congruous with those of the artefact.

— Artefact customization for a specific system: a given artefact may only be usable against a specific model or class of sensor, based on an analysis of the sensor's artefact detection properties. Evaluations of artefact efficacy may be designed to assess a given artefact, artefact series, or artefact species against a specific sensor model or class.

— Biometric characteristic sourcing: artefacts may be based on direct or indirect representations of biometric samples or characteristics, on modified or manipulated biometric samples or characteristics, or on synthetic samples or biometric characteristics. The efficacy of derived artefacts may be a function of the performance of biometric samples or characteristics.

— Artefact creation and preparation cost: creation of an artefact will involve cost for sourcing the materials required and for manufacturing. A cheaper, reliable artefact and one that can be easily manufactured may be favoured.

Evaluations of PAD mechanisms and resulting reports shall describe how artefacts were created and prepared, addressing the following:

— creation and preparation processes;

— effort required to create and prepare artefacts (e.g. technical know-how, creation time, difficulty of collecting artefact materials, creation instruments, and preparation instruments);

— ability to consistently create and prepare artefacts with intended properties;

— customization of artefacts for specific capture subjects;

— customization of artefacts for specific systems;

— sourcing of biometric characteristics;

— availability of public information on creation and preparation process;

— changes in artefact creation or preparation processes over the course of the evaluation.

IECNORM.COM : Click to view the full PDF of ISO/IEC 30107-3:2017

 © ISO/IEC 2017 – All rights reserved

10.3 Artefact usage

In evaluations of PAD mechanisms where artefact-based presentation attack instruments are in use, the following factors and parameters should be taken into consideration:

— Artefact presentation training and habituation: the amount of training necessary to utilize and present an artefact, and the amount of training and habituation provided to the artefact presenter, may impact artefact efficacy. Certain types of artefacts may require little presentation training and habituation, such as a replay of an audio recording. Others may require substantial training and habituation, such as presentation of an artefact to a fingerprint swipe sensor.

— Artefact presentation durability: certain types of materials-based artefacts may have a finite utilization lifespan, such that their efficacy decreases after one or more presentations. Conversely, an ideal artefact would be infinitely reusable. Artefacts may be characterized by differences in time and number of presentations that result in acceptance of an artefact (e.g. a silicone fingerprint PAI is a more durable artefact than a gelatine PAI).

— Covert use of the artefact: successful use of artefact may depend on whether the application is supervised, and if so, the degree of scrutiny that might be applied during artefact usage.

Evaluations of PAD mechanisms and resulting reports shall describe how artefacts were used in the evaluation, addressing the following:

— level of attacker training and habituation;

— artefact durability, including the number of presentations associated with each artefact;

— level of scrutiny or oversight applied during artefact usage.

10.4 Iterative testing to identity effective artefacts

Based on the creation, preparation, and usage considerations above, an evaluator could evaluate presentation attack instruments with a special effort on those found to be initially effective. The analysis could take place in two phases. After a first phase of tests, the evaluator could test extensively each PAI misclassified as bona fide in a second phase of tests. APCER could then be measured for each selected PAI. If APCER exceeds a fixed threshold for one PAI species, the PAI would be deemed successful. Additionally, if a PAI does not cross the APCER threshold in the second phase of evaluation, the evaluator should still put special effort to determine if PAI effectiveness can be increased by refining the creation process or improving the presentation method.

The evaluator could report the number of tests performed in the second phase and the threshold used for APCER. A very stringent methodology would use a 0 % threshold for APCER, meaning every presentation attack which demonstrates capability to be misclassified at least two times is deemed successful, as the PAI already succeeded at least once in the first phase.

11 Process-dependent evaluation factors

11.1 Overview

Processes for enrolment, identification, and verification may impact evaluation design. Evaluations of PAD mechanisms and resulting reports shall describe whether evaluation design considered enrolment, identification, and/or verification processes, or alternatively whether evaluation design considered a generic biometric sub-system independent of a specific process.

IECNORM.COM : Click to view the full PDF of ISO/IEC 30107-3:2017

© ISO/IEC 2017 – All rights reserved

11.2 Evaluating the enrolment process

Biometric systems have special vulnerabilities during the process of enrolment, often necessitating the implementation of PAD mechanisms. These include:

1) enrolment by a data subject of the biometric characteristics of a different individual;

2) enrolment of synthetic biometric characteristics not from any individual;

3) enrolment of "universal" biometric characteristics common to all or many individuals;

4) enrolment of biometric characteristics that can be altered in a consistent fashion.

Enrolment processes are often more time-consuming than identification and verification processes, involving validation of documents or other materials used to establish evidence of identity. Enrolment processes are often supervised or monitored such that the use of artefacts or non-conformant capture attempts may be discovered by an operator. Such discovery may be through visual inspection of the capture subject or through review of biometric data shown to the operator (e.g. on a computer screen).

EXAMPLE A test can involve personnel acting as operators who determine whether potentially suspect presentations are taking place.

Enrolment processes may also implement more rigorous biometric quality checks than identification or verification processes, increasing the likelihood that a presentation attack is detected. Lastly, enrolment processes often involve presentation of a given biometric characteristic multiple times. This has implications for the longevity and visual plausibility of the artefact or non-conformant capture attempt.

Evaluations of PAD mechanisms and resulting reports that apply to enrolment processes shall describe the following:

— use of enrolment-specific quality thresholds or presentation policy;

— parameters of the enrolment transaction, including number and duration of presentations;

— level of operator oversight present in the process;

— manner in which operator functions were applied or emulated in the evaluation.

11.3 Evaluating the verification process

Verification processes are less likely to be attended than enrolment or identification processes, with implications for artefact usage and non-conformant capture attempt. Artefacts may not require a high level of visual plausibility, and capture subjects may be able to experiment with different levels of non-conformant capture attempts to induce false matches.

Evaluations of PAD mechanisms and resulting reports that apply to verification processes shall describe the following:

— use of quality thresholds and presentation policy;

— parameters of the verification transaction, including the number and duration of presentations;

— level of operator oversight present in the process;

— manner in which operator functions were applied or emulated in the evaluation.

11.4 Evaluating the identification process

Identification processes, like enrolment processes, are often supervised or monitored such that the use of artefacts or non-conformant capture attempts may be discovered by an operator. However, the level of scrutiny applied to a capture subject during identification processes is likely to be less than

IECNORM.COM : Click to view the full PDF of ISO/IEC 30107-3:2017

 © ISO/IEC 2017 – All rights reserved

that applied during enrolment. This may impact the level of visual plausibility that the artefact or non-conformant capture attempt needs to achieve.

An identification system may be designed to return candidates above a score threshold, though such a search may not return any candidates. Alternatively, an identification system may return the strongest candidate regardless of comparison score. The latter type of identification system requires higher degrees of non-conformance to induce a false negative identification.

Evaluations of PAD mechanisms and resulting reports that apply to identification processes shall describe the following:

— use of quality thresholds and presentation policy;

— parameters of the identification transaction, including the number and duration of presentations;

— configuration of system to perform negative or positive identification;

— whether capture subjects were enrolled in the databases against which identification took place;

— level of operator oversight present in the process;

— whether and how an operator adjudicates candidate identities returned by the system;

— manner in which operator functions were applied or emulated in the evaluation.

11.5 Evaluating offline PAD mechanisms

Some outcomes of PAD mechanisms may not occur immediately after presentation, but offline at a later time. This may be necessary for a number of reasons including:

— PAD mechanisms may be time-consuming such that real-time processing of results is not feasible. Results could occur hours or days after the biometric presentation.

— Newer or different PAD mechanisms may be run across previously captured biometric samples.

— Subsequent events may suggest or confirm that a presentation attack has occurred. This may require evidence in the form of original biometric sample(s) to be retained for forensic analysis to detect and confirm PAD mechanism results and/or for court purposes.

Evaluation of offline PAD mechanisms might benefit from PAD mechanism data produced during a presentation and retained; ISO/IEC 30107-2 establishes requirements on such data.

Reports that evaluate offline PAD mechanisms shall describe their implementation in the overall processing scheme.

12 Evaluation using Common Criteria framework

12.1 General

The Common Criteria (ISO/IEC 15408-1[1], ISO/IEC 15408-2[2] and ISO/IEC 15408-3[3]) and the Common Evaluation Methodology (ISO/IEC 18045[4]) are relevant standards for independent security evaluation of IT products. The independent evaluation and certification of IT products according to these standards is widely used in many different areas. The Common Criteria standard is defined in three parts:

— ISO/IEC 15408-1 contains the “introduction and general model”;

— ISO/IEC 15408-2 contains the “security functional components”;

— ISO/IEC 15408-3 contains the “security assurance components”.

IECNORM.COM : Click to view the full PDF of ISO/IEC 30107-3:2017

© ISO/IEC 2017 – All rights reserved

The Common Evaluation Methodology[4] is a companion document to the Common Criteria standard and defines the minimum actions to be performed by an evaluator in order to conduct a Common Criteria evaluation, using the criteria and evaluation evidence defined in the Common Criteria standard.

Within the Common Criteria, the target of evaluation (TOE) is the IT product that is the subject of the evaluation. This corresponds to the IUT as referred to in this document. The TOE is characterized through the Security Target, a document that identifies the security functional requirements and security assurance requirements and may refer to one or more Protection Profiles. A Protection Profile is used to describe a class of IT products that share a certain scope and can be used to solve a certain security problem. A Security Target, on the other hand, describes the security characteristics of a concrete IT product and how it fulfils all security requirements.

Security functional components as defined in ISO/IEC 15408-2[2] are the basis for the security functional requirements expressed in a Protection Profile or Security Target. A Protection Profile or Security Target contains a set of security functional requirements to describe the security functionality of the TOE in a semi-formal language. The fact that the security functionality of a TOE is not only described in natural language but also in a semi-formal language serves to make different evaluations comparable.

The security assurance components determine the level of depth during evaluation. Every security assurance component from ISO/IEC 15408-3[3] stands for one task of the evaluator during evaluation. The seven predefined Evaluation Assurance Levels (EAL1 to EAL7) correspond to increasing efforts for design verification and testing as shown in Table 2.

Table 2 — EALs and their description

Evaluation Assurance Level (EAL)	Depth of evaluation
EAL1	Functionally tested
EAL2	Structurally tested
EAL3	Methodically tested and checked
EAL4	Methodically designed, tested and reviewed
EAL5	Semi-formally designed and tested
EAL6	Semi-formally verified, design and tested
EAL7	Formally verified, designed and tested

Each EAL includes a vulnerability assessment. Higher EAL reflects more rigorous vulnerability assessment and higher attack potential to be performed in penetration testing. Attack potential is a measure of the effort expended in the preparation and execution of the attack. The Common Evaluation Methodology gives general guidance on calculating attack potential as a function of required time, expertise, knowledge of the TOE, window of opportunity, and equipment.

A Protection Profile or Security Target includes the set of security assurance components predefined for an EAL, possibly augmented by additional assurance components.

The Common Criteria Recognition Arrangement (CCRA) has international certificate authorizing members and is further described under www.commoncriteriaportal.org. Protection Profiles for biometric systems are also listed on this website.

The Common Criteria framework is a pure security evaluation standard. In principle, the Common Criteria only focuses on the question whether an IT product provides the security functionality required for a certain use case/environment and whether sufficient trust can be laid into the implementation of this security functionality.

IECNORM.COM : Click to view the full PDF of ISO/IEC 30107-3:2017

© ISO/IEC 2017 – All rights reserved

12.2 Common Criteria and biometrics

12.2.1 Overview

Biometric systems can be evaluated according to the Common Criteria as any other IT product. Biometric systems have certain characteristics that need special consideration during an evaluation, including the following:

— **Biometric performance error rates:** Biometric authentication does not work as deterministically as other means for authentication or identification of users. Some biometric performance error rates (e.g. according to ISO/IEC 19795-1) have an impact on the security of the system and need to be considered during a security evaluation.

— **PAD:** It is well known that some biometric systems (e.g. PAD subsystem, data capture subsystem, or full system) may be vulnerable against presentation attacks. The evaluation of the capability to detect and defeat these attacks may belong into the scope of a Common Criteria evaluation depending on the use case of the TOE.

— **Vulnerability assessment:** Biometric systems in general may be subject to special kind of attacks (such as hill climbing) that will need consideration during a security evaluation.

For these areas, special guidance is required in order to facilitate a comparable evaluation in all laboratories of the Common Criteria schema worldwide. Special characteristics of biometrics in Common Criteria evaluations are dealt with in form of guidance for the evaluator performing an evaluation and the developer of a biometric system. ISO/IEC 19989[6], under development in ISO/IEC JTC 1/SC 27, provides such guidance. The most important aspects are summarized below in 12.2.2 to 12.2.5. Other approaches to security evaluation of biometrics are given in ISO/IEC 19792[5].

12.2.2 General evaluation aspects

The Common Criteria poses requirements on a wide variety of aspects of the TOE, starting from the development (including the development environment) up to the delivery of the TOE to the customer. Most aspects can be applied to biometric systems as to any other IT product. However, in some areas, specific guidance is given to the evaluator on how to evaluate these aspects. For example, the description of the design of a biometric system refers to specific aspects of the technology.

12.2.3 Error rates in testing

When it comes to testing a biometric system in the context of a Common Criteria evaluation, the security-relevant error rates are a very important aspect of the functionality to be considered. According to the guidelines, the evaluator will perform the following steps:

— **Identify the relevant test approach:** Various test approaches are available starting from a database-based technology test of a biometric algorithm to an evaluation of the performance of the biometric system under operation. The correct test approach highly depends on the definition of the TOE.

— **Identify the security-relevant error rates:** As Common Criteria focuses on the security-relevant error rates only, not all error rates of the biometric system are relevant. The identification of the security-relevant error rates is performed based on the type of the biometric system and its use case as defined in the Security Target.

— **Plan the execution of the test:** The actual test execution has to be planned and described within the test documentation in advance.

— **Estimate test size:** Collecting test data takes a significant amount of the effort of the overall test. It is essential to develop an idea about the amount of test data that is required before starting the actual process of test data acquisition.

— **Document the test plan:** It is essential to plan the required documentation for the test in advance of the test itself.

IECNORM.COM : Click to view the full PDF of ISO/IEC 30107-3:2017

© ISO/IEC 2017 – All rights reserved

— **Acquire test crew:** For the quality of results, it is essential that the evaluator utilizes a test crew not known to the developer of the system beforehand.

— **Perform test:** The test is carried out under the sole control and responsibility of the evaluator.

— **Evaluate test results:** After testing, results will be evaluated and reported according to defined metrics.

12.2.4 PAD evaluation

The Common Criteria itself does not require that a biometric system under evaluation provide PAD mechanisms. The requirement for PAD mechanisms is dependent on the intended environment of the biometric system.

For example, a border control system under the strong and constant control of a border control officer may not require PAD, while an ATM that uses biometrics as the only means for authentication would typically require PAD. The guidelines for the evaluation of biometrics, however, specify that PAD mechanisms, if existing, belong to the security functionality of the system and therefore are to be evaluated. In other words, it is not possible to evaluate a biometric system according to Common Criteria without consideration of its PAD functionality.

PAD mechanisms can be viewed from two perspectives:

— PAD mechanisms belong to the security functionality of the biometric system and are functionally tested. Guidelines direct the evaluator on how to plan, conduct, document, and evaluate such a functional test.

— PAD mechanisms also fall into the area of vulnerability assessment, as the use of a PAI against the biometric system is an attempt to circumvent the security functionality of the TOE.

The differences between the two perspectives can best be visualized using a concrete example. In the area of functional testing, the evaluators' concern regarding PAD is to verify that the TOE meets certain performance requirements. The PAD mechanism has to perform within a certain range of performance. Testing can be achieved by the use of a standardized toolbox. Beside some dedicated requirements on testing and documentation, this situation is very close to the situation in classical performance testing. Having passed the test from a functional perspective is a prerequisite to start the vulnerability assessment. If the PAD mechanisms would not work within sufficient performance limitations, any kind of vulnerability assessment would be useless. In the vulnerability assessment, the evaluator will then try to circumvent the PAD mechanism, working within the limitations of the attack potential of the current evaluation. This can lead to a situation in which a TOE passes the functional test but where the evaluator can build a so-called "golden fake" that reproducibly breaches the security functionality of the TOE. If this happens, the TOE fails the security evaluation even though it showed good performance during functional testing.

As a basic rule, it can be said that one successful attack against a TOE (always under consideration of the maximum attack potential) will make the security evaluation fail. This is one of the major differences of a security evaluation compared to a pure performance test.

12.2.5 Vulnerability assessment

12.2.5.1 Typical attack scenarios

Specific kinds of attacks against biometric systems exist. Presentation attacks are only one very prominent example. Also, for example, a biometric system can be vulnerable against a hill-climbing attack.

It is important that the evaluator considers typical and well-known presentation attacks during the evaluation of a biometric system. While the system is not necessarily vulnerable to all attacks, as a starting point for a vulnerability analysis, it is important that all typical attacks are considered. These can be seen as a minimum list of attacks to be considered. They do not claim to be complete and the evaluator will, in any case, develop additional attack scenarios during evaluation.

IECNORM.COM : Click to view the full PDF of ISO/IEC 30107-3:2017

 © ISO/IEC 2017 – All rights reserved

12.2.5.2 Rating attacks

Guidance for the security evaluation of biometric systems introduces a dedicated scheme to rate the attack potential of attacks against biometric systems as minimal, basic, enhanced-basic, moderate, high, or beyond high. The level chosen for the vulnerability analysis is one of the most important aspects of the chosen EAL. This decision basically answers the question against which attack potential a TOE is expected to be resistant.

The evaluator will perform their vulnerability assessment and penetration testing "only" up to the chosen level. Common Criteria uses a dedicated list of criteria to classify an attack in general. To reflect the dedicated characteristics of attacks against biometric systems, an extension and interpretation of the standard attack rating scheme have been proposed by the European Biometric Evaluation and Testing (BEAT) project[9]. This scheme uses the characteristics of elapsed time, expertise, knowledge about the TOE, access to the TOE/window of opportunity, access to the biometric characteristic, and success rate. The scheme utilizes a system of points to establish a numerical value for each attack. It also distinguishes between effort required to prepare/identify an attack and to exploit the attack. Such dedicated schemes for rating attacks have been proposed for other technical areas – namely smart cards and similar devices – in the past and are well accepted in the Common Criteria community.

12.2.5.3 Previous approaches in fingerprint PAD protection profiles

Many aspects of the methodology outlined above have their origin in an approach developed by the German Federal Office for Information Security (BSI). The BSI developed two dedicated Fingerprint Spoof Detection Protection Profiles[10][11] in order to describe the security characteristics of a biometric system with PAD mechanisms. Both Protection Profiles define the identical set of security functional requirements that have to be met by a TOE claimed to be compliant to the Protection Profile, namely:

— PAD (i.e. spoof detection);

— audit for security relevant events;

— protection of residual information;

— management of security functions.

Along with the Protection Profiles, a guideline has been developed[12] that provides guidance to the evaluator on how to evaluate PAD mechanisms. In the meantime, this guidance has been fed into the standardization activities within ISO/IEC JTC 1/SC 27 and has been used as the foundation of ISO/IEC 19989.

13 Metrics for the evaluation of biometric systems with PAD mechanisms

13.1 General

PAD mechanism performance can be expressed in terms of classification error rates, non-response rates, and other rate-based metrics. Such metrics could be utilized in security evaluations, academic evaluations, systematic technology or product development processes, or quick-look benchmarks by an end user. ISO/IEC 19795-1 provides an overview of the reporting requirements for a biometric performance test for bona fide presentations.

Evaluations of PAD mechanisms shall report the following:

— number of presentation attack instruments, PAI species, and PAI series used in the evaluation;

— number of test subjects involved in the testing, including those unable to utilize artefacts or present non-conformant characteristics;

— number of artefacts created per test subject for each material tested;

— number of sources from which artefact characteristics were derived;

IECNORM.COM : Click to view the full PDF of ISO/IEC 30107-3:2017

© ISO/IEC 2017 – All rights reserved

— number of tested materials;

— description of output information available from PAD mechanism;

— ordering of subject presentations with and without PAI, and whether subjects were reused;

— ordering of subject presentations to the PAD enabled and disabled system, and whether subjects were reused.

NOTE Performance metrics discussed in Clause 13 can fail to achieve statistical significance due to limitations in sample size.

13.2 Metrics for PAD subsystem evaluation

13.2.1 General

PAD subsystem evaluations (see ISO/IEC 30107-1:2016, Figure 4) measure the ability of PAD subsystems to correctly classify presentation attacks.

13.2.2 Classification metrics

Both APCER and BPCER are reported in PAD subsystem evaluations.

In PAD subsystem evaluations, performance metrics for presentation attacks shall be calculated and reported as APCER. The evaluator shall report on the manner in which PAD decisions and scores were used to classify presentations.

The APCER for a given PAI species, PAIS, shall be calculated using Formula (1):

$$\mathrm{APCER}_{\mathrm{PAIS}} = 1 - \left(\frac{1}{N_{\mathrm{PAIS}}} \right) \sum_{i=1}^{N_{\mathrm{PAIS}}} Res_i \tag{1}$$

where

N_{PAIS} is the number of attack presentations for the given PAI species;

Res_i takes value 1 if the ith presentation is classified as an attack presentation and value 0 if classified as a bona fide presentation.

Evaluations of PAD mechanisms shall report the number of artefact presentations correctly and incorrectly classified: total, by PAI species, by PAI series, by capture subject, and by source.

When considering how well a PAD subsystem performs in detecting PAI species of a specified attack potential AP, the APCER of the most successful PAI species within this attack potential should be used as shown in Formula (2):

$$\mathrm{APCER}_{\mathrm{AP}} = \max_{\mathrm{PAIS} \in A_{\mathrm{AP}}} \left(\mathrm{APCER}_{\mathrm{PAIS}} \right) \tag{2}$$

where A_{AP} is a subset of PAI species with attack potential at or below AP.

IECNORM.COM : Click to view the full PDF of ISO/IEC 30107-3:2017

 © ISO/IEC 2017 – All rights reserved

Attack potential should be calculated based on ISO/IEC 19989, under development by ISO/IEC JTC 1/SC 27.

NOTE The max-based formula reflects the vulnerability of a PAD system to at least one attack at a tested attack potential level. This is a good assumption for applications when measuring PAD error rates for the purpose of making security decisions, where the expected attacker would attack the system using the PAI most likely to be effective (within their means). In addition, attackers may use PAIS that were not tested, and using the max error rate observed among a suite of tested PAIS is a more reliable security metric. In operations, this APCER statement would apply if attackers had the same attack potential as deployed by the test laboratory's experimenters. In operational cases, where attackers had less knowledge than the test laboratory, and they selected presentation attack instruments randomly, or on basis of ease of production, a lower APCER rate would be achieved than given in the formula above.

At the PAD subsystem level, performance metrics for the set of bona fide presentations captured with the evaluation target shall be calculated and reported as BPCER. BPCER shall be calculated using Formula (3):

$$\text{BPCER} = \frac{\sum_{i=1}^{N_{\text{BF}}} Res_i}{N_{\text{BF}}} \tag{3}$$

where

N_{BF} is the number of bona fide presentations;

Res_i takes value 1 if the ith presentation is classified as an attack presentation and value 0 if classified as a bona fide presentation.

Evaluations of PAD mechanisms shall report the number of bona fide presentations correctly and incorrectly classified – total and by capture subject.

If the PAD subsystem returns a multi-valued PAD score, the frequency distributions of the PAD scores should be reported for each PAI species and for bona fide presentations.

Reporting the aggregate of APCER and BPCER (e.g. half-total error rate) is not conformant with this document.

The classification performance of a PAD mechanism may be reported in a single figure as BPCER at a fixed APCER.

EXAMPLE One may report BPCER when APCER_{AP} is 5 % as BPCER20.

When interpreting the performance of a PAD subsystem, it is important to recognize that there may be presentation attack types, PAI species and factors which have not been tested. Therefore, the reported performance of a PAD subsystem does not provide any information regarding its effectiveness in detecting presentation attacks which have not been tested.

13.2.3 Non-response metrics

Taking into account supplier recommendations and the intended use-case scenario for the PAD subsystem, the evaluator shall define what constitutes a non-response and specify conditions under which a non-response contributes to the classification error rate.

EXAMPLE An evaluator might define a non-response as no appearance of a biometric image for 5 s after presentation of a biometric characteristic or PAI.

The evaluator shall report non-response rates for the PAD subsystem using the following metrics:

— for each PAI species, attack presentation non-response rate (APNRR) and the sample size on which the computed rate is based;

— bona fide presentation non-response rate (BPNRR) and the sample size on which the computed rate is based.

IECNORM.COM : Click to view the full PDF of ISO/IEC 30107-3:2017

© ISO/IEC 2017 – All rights reserved

13.2.4 Efficiency metrics

Time-sensitive applications may be adversely affected by increased transaction time. The evaluator should report PAD subsystem processing duration (PS-PD) as mean duration. PS-PD should be reported separately for attack presentations and bona fide presentations. Non-responses are not included when calculating PS-PD. PS-PD may be determined by direct observation. Alternatively, the average processing duration change due to the PAD subsystem may be estimated by recording a number of presentations with and without PAD enabled and analysing the differences in processing durations.

13.2.5 Summary

Table 3 lists performance metrics for PAD subsystem evaluation.

Table 3 — PAD subsystem performance metrics

Subsystem	Metric	Type of presentation	Reporting
PAD subsystem	APCER	Attack	Mandatory
	BPCER	Bona fide	Mandatory
	APNRR	Attack	Mandatory
	BPNRR	Bona fide	Mandatory
	PS-PD	Bona fide or attack	Optional

For PAD subsystems that return a multi-valued PAD score, PAD score frequency distributions are recommended for each PAI species and for bona fide presentations.

13.3 Metrics for data capture subsystem evaluation

13.3.1 General

Data capture subsystem evaluations measure the ability of the subsystem to correctly classify presentation attacks.

13.3.2 Classification metrics

In data capture subsystem evaluations, performance metrics for presentation attacks shall be calculated and reported as APCER and BPCER.

Taking into account supplier recommendations and intended use-case scenario for the device, the evaluator shall define what constitutes a non-response and specify conditions under which a non-response contributes to the classification error rate.

A presentation attack correctly classified by the quality system is treated as successful presentation attack detection and contributes to the denominator of APCER.

13.3.3 Non-response and capture metrics

The evaluator shall report non-response rates of the data capture subsystem using the following metrics:

— for each PAI species, APNRR and the sample size on which the computed rate is based;

— BPNRR and the sample size on which the computed rate is based.

The evaluator shall report capture rates of the data capture subsystem using the following metrics:

— for each PAI species, attack presentation acquisition rate (APAR) and the sample size on which the computed rate is based;

IECNORM.COM : Click to view the full PDF of ISO/IEC 30107-3:2017

© ISO/IEC 2017 – All rights reserved

— for bona fide capture subjects erroneously rejected by capture or quality sub-systems, FTA and/or FTE as defined in ISO/IEC 19795-1 and the sample size on which the computed rate is based.

FTE is reported for evaluations with an enrolment component. FTA is reported for evaluations with a recognition component.

13.3.4 Efficiency metrics

The evaluator should report data capture subsystem processing duration (DCS-PD) as mean duration. Data capture subsystem processing duration should be reported separately for attack presentations and bona fide presentations. Non-responses are not included when calculating DCS-PD.

NOTE Statistical evaluation can provide zero-normalized duration scores, as well as for each subject and over whole test crew population.

13.3.5 Summary

Table 4 lists performance metrics for data capture subsystem evaluation.

Table 4 — Data capture subsystem performance metrics

Subsystem	Metric	Type of presentation	Reporting
Data capture subsystem	APCER	Attack	Mandatory
	BPCER	Bona fide	Mandatory
	APNRR	Attack	Mandatory
	BPNRR	Bona fide	Mandatory
	APAR	Attack	Mandatory
	FTE	Bona fide	Mandatory
	FTA	Bona fide	Mandatory
	DCS-PD	Attack or bona fide	Optional

13.4 Metrics for full-system evaluation

13.4.1 General

Full-system evaluations include comparison subsystem results in addition to PAD or data capture subsystem results.

NOTE Depending on the IUT, PAD or data capture subsystem results may not be available.

13.4.2 Accuracy metrics

13.4.2.1 Evaluation of verification systems

For verification systems, for each PAI species, at least one of the following shall be reported:

— IAPMR and the sample size on which this computed rate is based;

— CAPNMR and the sample size on which this computed rate is based.

NOTE To defeat recognition, biometric concealers desire a high CAPNMR, as well as a high APCER. To be falsely recognized, biometric impostors desire a high IAPMR, as well as a high APCER.

If the evaluation includes both biometric impostors and biometric concealers, then both IAPMR and CAPNMR shall be reported.

IECNORM.COM : Click to view the full PDF of ISO/IEC 30107-3:2017

© ISO/IEC 2017 – All rights reserved

13.4.2.2 Evaluation of positive identification systems

For positive identification systems, for each PAI species, impostor attack presentation identification rate (IAPIR) and the sample size on which the computed rate is based shall be reported.

NOTE To be falsely recognized, biometric impostors desire a high IAPIR, as well as a high APCER.

13.4.2.3 Evaluation of negative identification systems

For negative identification systems, for each PAI species, concealer attack presentation non-identification rate (CAPNIR) and the sample size on which the computed rate is based shall be reported.

NOTE To defeat recognition, biometric concealers desire a high CAPNIR, as well as a high APCER.

13.4.3 Efficiency metrics

The evaluator should report full-system processing duration (FS-PD). Increases in FS-PD due to PAD may be important in high throughput and other time-sensitive applications. The time required for PAD characteristics to be processed by the signal processing subsystem may be different than for bona fide biometric characteristics. FS-PD accounts for changes in signal processing durations due to PAD mechanisms along with durations accumulated across all other subsystems.

FS-PD with PAD mechanisms enabled and disabled should also be reported. FS-PD may be determined by direct observation. Alternatively, an aggregate average processing duration increase due to PAD mechanisms may be estimated by recording a number of transactions with and without PAD mechanisms enabled and analysing the differences in processing durations.

13.4.4 Summary

Table 5 lists performance metrics for full-system evaluation.

Table 5 — Full-system performance metrics

Subsystem (recognition type)	Metric	Type of presentation	Reporting
Comparison subsystem (verification)	FNMR/FMR	Bona fide	Mandatory
	IAPMR	Attack	Mandatory for biometric impostors
	CAPNMR	Attack	Mandatory for biometric concealers
	FS-PD	Attack or bona fide	Optional
Comparison subsystem (positive identification, applicable to biometric impostors)	FPIR	Bona fide	Mandatory
	IAPIR	Attack	Mandatory
	FS-PD	Attack or bona fide	Optional
Comparison subsystem (negative identification, applicable to biometric concealers)	FNIR	Bona fide	Mandatory
	CAPNIR	Attack	Mandatory
	FS-PD	Attack or bona fide	Optional

IECNORM.COM : Click to view the full PDF of ISO/IEC 30107-3:2017

© ISO/IEC 2017 – All rights reserved

Annex A
(informative)

Classification of attack types

A.1 Overview

This annex provides a classification and brief description of known presentation attack types, as outlined in Table A.1. The purpose of this annex is to provide a foundation for structured evaluation of countermeasures. In this way, an assessment of a countermeasure can be empirically tested and answer the question, "How effectively does this countermeasure classify attacks?" An assessment of countermeasures based on known attacks establishes the rationale for making a substantial security claim about a product.

This annex is not a recipe book for making biometric artefacts. Attacks are described at a high level and classified, but this should not be considered as a comprehensive listing.

Presentation attacks are divided into two categories: those based on artificial presentation attack instruments and those based on human presentation attack instruments.

A.2 Use of artificial presentation attack instruments

Source of biometric characteristics. An artificial PAI, or artefact, is formed based on a source of the biometric characteristics (see Table A.1). Biometric characteristics can be recorded or copied onto artificial objects. In this type of attack, the attacker should have access to a representation of the original biometric characteristics, either directly (cooperatively or coerced from a victim), indirectly from latent traces, or from images or other recordings. A PAI can also be synthetically generated to represent a biometric characteristic. The synthetic data may be prepared in several ways:

a) generated without a requirement to resemble biometric characteristics of a human, based on:
   - random generation of biometric characteristics' elements;
   - alterations or amalgamations of existing biometric characteristics;
   - reverse engineering of coding methods without taking into account resemblance to a characteristic of a subject;

b) generated so as to resemble biometric characteristics of any subject, based on:
   - alterations or amalgamations of existing biometric characteristics without introducing abnormalities;
   - reverse engineering of coding methods with additional limitations on the generation effect;

c) generated so as to resemble biometric characteristics of a specific subject, based on reverse engineering of coding methods with additional limitations on the generation effect given the biometric template.

An artificial presentation attack may not have a source for the biometric characteristic, particularly where the goal may be to obscure one's identity through masking (e.g. ski mask, opaque contact lens) or through creating a different identity where no particular biometric characteristics are desired (e.g. make-up, prosthetic). Generation of synthesized yet realistic biometric characteristics may be difficult or impossible for selected modalities since it requires a set of machine-programmed rules that define attributes of a real human body part or a real human behaviour.

IECNORM.COM : Click to view the full PDF of ISO/IEC 30107-3:2017

© ISO/IEC 2017 – All rights reserved