INTERNATIONAL STANDARD

ISO/IEC 19989-3

First edition
2020-09

Information security — Criteria and methodology for security evaluation of biometric systems —

Part 3: Presentation attack detection

Sécurité de l'information — Critères et méthodologie pour l'évaluation de la sécurité des systèmes biométriques —

Partie 3: Détection d'attaque de présentation

Reference number
ISO/IEC 19989-3:2020(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

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 ISO documents 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 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 of 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 www.iso.org/iso/foreword.html.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

A list of all parts in the ISO/IEC 19989 series can be found on the ISO website.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

Biometric systems can be vulnerable to presentation attacks where attackers attempt to subvert the system security policy by presenting their natural biometric characteristics or artefacts holding copied or faked characteristics. Presentation attacks can occur during enrolment or identification/verification events. Techniques designed to detect presentation artefacts are generally different from those to detect attacks where natural characteristics are used. Defence against presentation attacks with natural characteristics typically relies on the ability of a biometric system to discriminate between genuine enrolees and attackers based on the differences between their natural biometric characteristics. This ability is characterized by the biometric recognition performance of the system. Biometric recognition performance and presentation attack detection have a bearing on the security of biometric systems. Hence, the evaluation of these aspects of performance from a security viewpoint will become important considerations for the procurement of biometric products and systems.

Biometric products and systems share many of the properties of other IT products and systems which are amenable to security evaluation using the ISO/IEC 15408 series and ISO/IEC 18045 in the regular way. However, biometric systems embody certain functionality that needs specialized evaluation criteria and methodology which is not addressed by the ISO/IEC 15408 series and ISO/IEC 18045. Mainly, these relate to the evaluation of biometric recognition and presentation attack detection. These are the functions addressed in this document.

ISO/IEC 19792 describes these biometric-specific aspects and specifies principles to be considered during the security evaluation of biometric systems. However, it does not specify the concrete criteria and methodology that are needed for security evaluation based on the ISO/IEC 15408 series.

The ISO/IEC 19989 series provides a bridge between the evaluation principles for biometric products and systems defined in ISO/IEC 19792 and the criteria and methodology requirements for security evaluation based on the ISO/IEC 15408 series. The ISO/IEC 19989 series supplements the ISO/IEC 15408 series and ISO/IEC 18045 by providing extended security functional requirements together with assurance activities related to these requirements. The extensions to the requirements and assurance activities found in the ISO/IEC 15408 series and ISO/IEC 18045 relate to the evaluation of biometric recognition and presentation attack detection which are particular to biometric systems.

This document provides guidance and requirements to the developer and the evaluator for the supplementary activities on presentation attack detection specified in ISO/IEC 19989-1. It builds on the general considerations described in ISO/IEC 19792 and the presentation attack detection testing methodology described in ISO/IEC 30107-3 by providing additional guidance to the evaluator.

In this document, the term "user" is used to mean the term "capture subject" used in biometrics.

Information security — Criteria and methodology for security evaluation of biometric systems —

Part 3: Presentation attack detection

1 Scope

For security evaluation of biometric verification systems and biometric identification systems, this document is dedicated to security evaluation of presentation attack detection applying the ISO/IEC 15408 series. It provides recommendations and requirements to the developer and the evaluator for the supplementary activities on presentation attack detection specified in ISO/IEC 19989-1.

This document is applicable only to TOEs for single biometric characteristic type but for the selection of a characteristic from multiple characteristics.

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 15408-3:2008, *Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance components*

ISO/IEC 18045:2008, *Information technology — Security techniques — Methodology for IT security evaluation*

ISO/IEC 19989-1:2020 *Information Technology — Security techniques — Criteria and methodology for security evaluation of biometric systems – Part 1: framework*

ISO/IEC 30107-3:2017, *Information technology — Biometric presentation attack detection — Part 3: Testing and reporting*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

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

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

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

3.1
attack presentation acquisition rate
APAR
proportion of attack presentations using the same *PAI species* (3.15) from which the data capture subsystem acquires a biometric sample of sufficient quality

[SOURCE: ISO/IEC 30107-3: 2017, 3.2.5]

3.2
attack presentation classification error rate
APCER
proportion of attack presentations using the same *PAI species* (3.15) incorrectly classified as *bona fide presentations* (3.5) in a specific scenario

[SOURCE: ISO/IEC 30107-3: 2017, 3.2.1]

3.3
attack presentation non-response rate
APNRR
proportion of attack presentations using the same *PAI species* (3.15) 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.

[SOURCE: ISO/IEC 30107-3: 2017, 3.2.3]

3.4
attack type
element and characteristic of a presentation attack, including *PAI species* (3.15), concealer or impostor attack, degree of supervision, and method of interaction with the capture device

[SOURCE: ISO/IEC 30107-3: 2017, 3.1.3]

3.5
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.

[SOURCE: ISO/IEC 30107-3: 2017, 3.1.2]

3.6
bona fide presentation classification error rate
BPCER
proportion of *bona fide presentations* (3.5) incorrectly classified as presentation attacks in a specific scenario

[SOURCE: ISO/IEC 30107-3: 2017, 3.2.2]

3.7
bona fide presentation non-response rate
BPNRR
proportion of *bona fide presentations* (3.5) that cause no response at the PAD subsystem or data capture subsystem

[SOURCE: ISO/IEC 30107-3: 2017, 3.2.4]

3.8
concealer attack presentation non-identification rate
CAPNIR
<full-system evaluation of an identification system> proportion of concealer presentation attacks using the same *PAI species* (3.15) 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 can intend that no identifiers are returned to avoid scrutiny by a human operator.

[SOURCE: ISO/IEC 30107-3: 2017, 3.2.9]

3.9
concealer attack presentation non-match rate
CAPNMR
<full-system evaluation of a verification system> proportion of concealer attack presentations using the same *PAI species* (3.15) in which the reference of the concealer is not matched

[SOURCE: ISO/IEC 30107-3: 2017, 3.2.7]

3.10
false-negative identification-error rate
FNIR
proportion of identification transactions by users enrolled in the system in which the user's correct identifier is not among those returned

[SOURCE: ISO/IEC 19795-1:2006, 4.6.8]

3.11
false-positive identification-error rate
FPIR
proportion of identification transactions by users not enrolled in the system, where an identifier is returned

[SOURCE: ISO/IEC 19795-1:2006, 4.6.9]

3.12
impostor attack presentation identification rate
IAPIR
<full-system evaluation of an identification system> proportion of impostor attack presentations using the same *PAI species* (3.15) 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 can be both an impostor (trying to match an existing non-self enrolee) and a concealer (obscuring his real biometric sample with a PAI).

[SOURCE: ISO/IEC 30107-3: 2017, 3.2.8]

3.13
impostor attack presentation match rate
IAPMR
<full-system evaluation of a verification system> proportion of impostor attack presentations using the same *PAI species* (3.15) in which the target reference is matched

[SOURCE: ISO/IEC 30107-3: 2017, 3.2.6]

3.14
non-standard PAI
presentation attack instrument (PAI) not corresponding to a *standard PAI species* (3.18).

3.15
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.

[SOURCE: ISO/IEC 30107-3: 2017, 3.1.6]

3.16
penetration testing
testing used in vulnerability analysis for vulnerability assessment, trying to reveal vulnerabilities of the TOE based on the information about the TOE gathered during the relevant evaluation activities

Note 1 to entry: In the ISO/IEC 15408 series, this term is used without definition.

3.17
standard PAI
PAI in *standard PAI species* (3.18)

3.18
standard PAI species
PAI species (3.15) determined and specified as standard by a certification body or a technical community for the purpose of conducting evaluations

Note 1 to entry: If standard PAI species are not specified, the developer as well as the evaluator prepare *non-standard PAIs* (3.14) to use in evaluation activities.

4 Abbreviated terms

ADV	security assurance requirement (SAR) class of development
	NOTE The class name is defined in ISO/IEC 15408-3. Here, A stands for assurance requirement, DV for development. The class name is defined in this way in ISO/IEC 15408.
ATE	security assurance requirement (SAR) class of tests
AVA	security assurance requirement (SAR) class of vulnerability assessment
AVA_VAN	security assurance requirement (SAR) family for vulnerability analysis in class AVA
FMR	false match rate
FNIR	false-negative identification-error rate
FNMR	false non-match rate
FPIR	false-positive identification-error rate
FTAR	failure to acquire rate
FTER	failure to enrol rate

PAD	presentation attack detectioin
PAI	presentation attack instrument
PP	protection profile
SFR	security functional requirement
ST	security target
TOE	target of evaluation

5 General remark

In addition to the requirements and recommendations provided in this document, those in ISO/IEC 15408-3 and ISO/IEC 18045 shall be applied.

The definition of authentication is available in ISO/IEC 2382.

The definitions of biometric (adjective), biometric capture, biometric capture device, biometric characteristic, biometric concealer, biometric enrolment, biometric identification, biometric impostor, biometric recognition, biometric system, biometric verification, comparison, enrol, failure-to-acquire rate, failure-to-enrol rate, false match rate, false non-match rate, identify and threshold (noun) are available in ISO/IEC 2382-37.

NOTE 1 In this document, the expression "capture device" is sometimes used instead of "biometric capture device".

NOTE 2 In this document, the expression "concealer" is sometimes used instead of "biometric concealer".

NOTE 3 In this document, the expression "enrolment" is sometimes used instead of "biometric enrolment".

NOTE 4 In this document, the expression "impostor" is sometimes used instead of "biometric impostor".

The definition of assurance, attack potential, class, component, confirm, delivery, describe, determine, developer, development, ensure, evaluation, family, Protection Profile, Security Target, target of evaluation and vulnerability are available in ISO/IEC 15408-1.

The definitions of activity, methodology and report are available in ISO/IEC 18045:2008.

The definitions of presentation attack, presentation attack detection and presentation attack instrument are available in ISO/IEC 30107-1.

6 Overview of PAD testing in Class ATE and Class AVA

6.1 Objectives and principles

6.1.1 Class ATE

The activities in Class ATE focus on the question whether the provided PAD mechanisms work as specified. Functional testing can demonstrate the existence of PAD vulnerabilities in the TOE (i.e. non-zero error rates) but it cannot prove that no vulnerabilities exist.

Functional testing of the effectiveness of the PAD capability of the TOE is done by measuring the successes and failures of detection by the TOE of PAIs using a statistically based test methodology (i.e. the measurement of PAD success and error rates), in order to demonstrate that PAD capability exists and that the PAD error rates meet the specification in the ATE_FUN documentation. ATE_IND may or may not include statistical testing depending on the evaluation context.

Note that the functional testing described in this document is distinct from the functional testing of biometric recognition performance using the natural biometric characteristics of test subjects described in ISO/IEC 19989-2 following intended use of the TOE.

6.1.2 Class AVA

Class AVA evaluation includes penetration testing activities. Penetration testing involves investigating the potential vulnerabilities of a TOE to presentation attacks which may not have been uncovered by previous functional testing (class ATE). This can include standard PAIs and variants of standard PAIs used in functional testing, and new PAIs which are created to expose possible PAD weaknesses in the capture hardware or software algorithms used, for example, in signal processing and biometric comparison. Penetration testing does not involve the statistical testing approach used for functional testing (class ATE).

Note that testing with PAIs is subject to presentation variability and PAI preparation variability. Testing should be continued until an appropriate level of confidence in the results of the test is achieved corresponding to the level of the assurance family AVA_VAN specified in the ST of the TOE.

6.2 PAIs used in testing activities

6.2.1 Class ATE

Standard PAIs shall be prepared and used in accordance with specifications and instructions, if provided. Standard PAIs may be supplied to the developer and the evaluator by the certification body or a technical community, or prepared by the developer and the evaluator in accordance with specifications and instructions of the standard PAI species. If standard PAIs are not provided, then non-standards PAIs shall be constructed and used by the developer and the evaluator.

NOTE The use of natural biometrics as PAI is included in testing activities if SFR(s) such as FPT_BCP.1, FIA_EBR.1, FIA_BVR.4 and FIA_BID.4 specified in ISO/IEC 19989-1 are selected in the ST. Even if those SFRs are not selected, natural biometric PAIs can be part of the standard PAIs. As described in ISO/IEC 19989-1:2020, 6.4.2.1, 7.5.1.1, 7.5.6.1, and 7.5.10.1, natural biometric PAIs include natural biometric characteristics presented with movements, rotations, or distances against the specification of the capture device. This also applies to Class AVA.

If standard PAIs are not provided, non-standard PAIs shall be prepared by the developer and supplied to the evaluator by the developer.

The PAIs used by the evaluator for ATE vary with the information available to the evaluator because it is one of the key factors of the determination of the PAIs used by the evaluator. By default, the evaluator should rely on the standard PAI species. Additionally, the evaluator should rely on state-of-the-art attack information to determine whether the PAIs used for the functional testing are representative of the PAIs that can be used on the TOE by attackers.

6.2.2 Class AVA

Non-standard PAIs shall be created and used by the evaluator in penetration testing.

6.3 Testing activities

6.3.1 Class ATE

It is the objective of any functional testing activity conducted in Class ATE to determine whether the PAD mechanism is able to detect PAIs with sufficient reliability. In ATE_FUN.1 and ATE_FUN.2, the developer shall conduct functional testing using standard PAIs at least or non-standard PAIs depending on whether standard PAI species are provided or not. The developer may prepare non-standard PAIs to conduct additional functional testing which gives information on the nature of the PAIs the evaluator should focus on in order to reduce the evaluator's evaluation activities.

The evaluator shall conduct independent testing using PAIs selected from standard PAIs, if standard PAI species are provided, or non-standard PAIs.

The values for maximum error rates to be validated in the evaluation are specified in the TOE ATE_FUN documentation and the implications of the values to the test sizes are further discussed in 6.3.

The error rates shall be reported independently for each PAI species tested. The maximum error rate of all PAI species tested is the main indicator on how well the TOE performs in detecting given PAI species.

NOTE ADV documents are disclosed only to the evaluator and the certification body while the ST is publicized when the TOE is certified.

6.3.2 Class AVA

Functional testing clearly does not provide any information on the PAD effectiveness against untested PAI species. It falls to the vulnerability assessment to evaluate whether the use of additional PAIs that have not been part of the standard PAI species or variations of PAIs from the standard PAI species can lead to exploitable vulnerabilities.

During the vulnerability analysis, the evaluator should use information and knowledge gained during the evaluation of the other assurance classes for penetration testing. Any information found in the previous evaluation activities shall be made available as input to the activities for the AVA evaluation activities described in this document.

Penetration testing depends on the evaluator's expertise, skill, and knowledge on potential PAD vulnerabilities, such as identification of possible areas of weakness, iteratively probing these areas using specially prepared PAIs, refining the PAIs, and the presentation techniques to attempt to find vulnerabilities, based on public and private sources of information available on vulnerabilities and PAIs. Penetration testing is characterized as an activity based on knowledge, expertise, skill and learning to penetrate the TOE using specific PAIs for which the attack potential is calculated from associated information such as expertise, effort, time, cost, etc., needed by the evaluator to identify and exploit the vulnerabilities.

NOTE Penetration testing cannot prove that no vulnerabilities exist even if it fails to uncover any PAD vulnerabilities in the TOE.

6.4 Criteria of pass/failure

The TOE shall pass the evaluation only if:

— the functional testing shows that the TOE is able to recognize the PAIs within the maximum error rates stated in the TOE ATE_FUN documentation; and

— the vulnerability analysis shows that dedicated variations of standard PAIs or any other innovative non-standard PAIs designed by the evaluator do not lead to vulnerabilities with an attack below the considered attack potential.

7 Supplementary activities to ISO/IEC 18045 on tests (ATE)

7.1 Testing approach toward PAD

The main objective of the testing activity for PAD systems is to demonstrate that the PAD mechanism is able to detect presentation attacks with sufficient reliability. To achieve this, the developer shall determine the rate at which the TOE fails to detect PAIs of a given PAI species – the attack presentation classification error rate (APCER) for that PAI species.

In order to determine the APCER of the PAD mechanism, the developer shall prepare standard PAIs if provided.

In the course of their testing activity, the PAIs prepared by the developer shall be presented to the PAD system and the resulting PAD decision (presentation attack detected/presentation attack not detected) shall be recorded. The developer shall prepare and test using the standard PAI species applicable to the TOE and may extend the testing to include non-standard PAIs.

In order to judge whether or not a PAD mechanism is working adequately, the maximum values for APCER and definitions for the minimal number of attack types and PAI species shall be defined in the TOE ATE_FUN documentation.

As required by ATE_IND.2 and ATE_IND.3, the evaluator shall repeat a subset of the developer tests and also devise their own tests in order to gain confidence in the testing activity of the developer. For the repetition of developer tests, the developer shall provide the description of their PAIs to the evaluation body. Additionally, the evaluation body shall create their own PAIs based on the more detailed information from the complete documentation of the standard PAI species provided. Therefore, independence and a sufficient degree of variation is given.

The maximum APCER and minimal test sizes as introduced above should also be considered for ATE_IND. The maximum APCER value shall separately be assigned to every PAI species and not only for the set of all prepared PAIs.

Summarizing, the developer and the evaluator shall both use the standard PAI species, if provided, as the basic set of PAIs for their testing activities. In this way it can be ensured that a representative set of PAIs is used to test the TOE. The documentation of the standard PAI species defines a minimum set of attack types that every system for PAD shall be able to detect. It does not only define PAI species but also defines concealer or impostor attack, degree of supervision and method of interaction with the capture device for each PAI. The document should be maintained and developed to keep track of the evolving threat scenario along with the needs of the market and the further development of PAD systems.

It is important to note that the testing approach described here is not sufficient to claim that the PAD mechanism cannot be circumvented by any other PAIs than those used for testing the TOE during the functional testing. This aspect is a part of the vulnerability analysis (AVA_VAN) which is discussed in Clause 7.

7.2 Metrics for PAD testing

7.2.1 General

The ISO/IEC 30107 series classifies presentation types in terms of the intention of the presenter, i.e. bona fide presentations and attack presentations. However, PAD systems are normally unable to determine a presenter's intent and PAD techniques are based on the measurement of physical and/or behavioural attributes associated with a presentation plus a decision scheme that classifies the presentation as either a bona fide presentation or an attack presentation. The PAD decision is not wholly deterministic and decision errors can occur in operational biometric systems where attack presentations are misclassified as bona fide or bona fide presentations are misclassified as attacks.

Recognizing this, ISO/IEC 30107-3 specifies a set of PAD metrics including error metrics that are defined for the bona fide and attack presentation types.

The metrics specified in ISO/IEC 30107-3 shall be used in ADV documentation, functional testing for PAD, and its documentation. The appropriate metrics depend on the functionality provided by the TOE. The error rates measured with the metrics shall be independently reported for each PAI tested.

ISO/IEC 30107-3 provides a number of metrics which can be used for testing the performance of PAD systems. Subclause 6.2 specifies the metrics of ISO/IEC 30107-3 that shall be used for PAD testing. The appropriate metrics depend on the functionality provided by the TOE.

7.2.2 Metrics used for PAD subsystem TOEs

PAD testing shall include the metrics APCER, BPCER, APNRR, and BPNRR, which are mandatory. In addition, PAD subsystem processing duration (PS-PD) from the PAD subsystem can be measured and reported as mean duration. Table 1 summarizes the relation among error rate, presentation type and attack classification. Note that the two metrics APNRR and BPNRR shall be evaluated under the PAD subsystem processing duration.

BPCER can be relevant to the performance and usability of a system because occurrences can cause usability problems and delays for affected users. Though ISO/IEC 15408 security evaluation primarily focusses on security rather than usability/performance issues, testing of the BPCER is necessary to determine whether the TOE is adequate for its purpose. As APCER and BPCER are dependent metrics and are usually tuned using specific parameters, the developer can easily decrease the APCER while increasing the BPCER. BPCER test conditions shall be the same as those for APCER.

APCER and BPCER error rate testing does not generally require the size of test crew that is normal for biometric performance testing because APCER and BPCER error rates for PAD systems are typically substantially greater than the FAR and FRR error rates for bona fide presentations and consequently the associated statistical uncertainty limits are less demanding. Note that, if the testing of biometric recognition performance of the TOE for bona fide presentations is also part of the evaluation, the BPCER figures can be derived from the results of that testing and reported as supplementary information in the document for the ATE_FUN activity.

NOTE APCER for a given PAI species PAIS is defined and denoted as $APCER_{PAIS}$ in ISO/IEC 30107-3.

Table 1 — Relation among error rates, presentation type, and attack classification for PAD subsystem

Presentation type (Input)	PAD result (Output)		
	Attack	Bona fide	No response
Attack	—	APCER	APNRR
Bona fide	BPCER	—	BPNRR
— Out of consideration.			

7.2.3 Metrics used for data capture subsystem TOEs

The used error metrics are APCER, BPCER, APNRR, BPNRR, APNCR, APAR, FTER, and FTAR which are mandatory. In addition, data capture subsystem processing duration may be used. Table 2 summarizes the relation among error rate, presentation type, and attack classification. Note that the above metrics should be evaluated within the time interval of the data capture subsystem processing duration.

NOTE A data capture subsystem, consisting of capture hardware or/and software, couples PAD mechanisms and quality checks which can be opaque to the evaluator. Therefore, the evaluator may not always know whether a failure results from a detection of a presentation attack or a poor quality of the biometric characteristics.

Table 2 — Relation among error rates, presentation type, and attack classification for data capture subsystem

Presentation type (Input)	PAD result (Output)					
	Attack	Bona fide	No response	Capture failure		Capture success
Attack	—	APCER	APNRR	—		APAR
Bona fide	BPCER	—	BPNRR	Enrolment	FTER	—
				Verification/ Identification	FTAR	—
— Out of consideration.						

7.2.4 Metrics used for other TOEs

Other TOEs correspond to the third case in ISO/IEC 19989-1:2020, 5.3.2. Such a TOE contains at least the comparison and decision subsystems for biometric verification or identification. This category of TOEs includes a full system. PAD evaluation to a TOE of this category, even if the TOE itself is not a full system, shall be done for a full system complementing other components to the TOE, if any, where the other components shall be specified in the ST.

When the TOE is for biometric verification, the metrics are FNMR, FMR, IAPMR for biometric impostors, and CAPNMR for biometric concealers. When the TOE is for positive identification, the metrics are FPIR and IAPIR. When the TOE is for negative identification, the metrics are FNIR and CAPNIR. All these metrics are mandatory (see ISO/IEC 19795-1 for FNMR, FMR, FNIR, and FPIR). In addition, full system processing duration is optionally used. The mandatory metrics should be evaluated within the time interval of the full system processing duration. Table 3 and Table 4 summarize the relation among error rate, presentation type, and attack classification.

If the concealer produces a match against a different subject, it shall be considered as a match by the impostor.

NOTE 1 If the TOE outputs the result of PAD in addition to the decision in some way, APCER and BPCER can be used.

Table 3 — Relation among error rates, presentation type, and attack classification for full system of biometric verification

Presentation type (Input)			Decision (Output)	
			Match	No match
PAI (natural biometric characteristic/artefact)	Attack presentation	Impostor	IAPMR	—
		Concealer	—	CAPNMR
Natural biometric characteristic		Impostor	FMR	—
	Bona fide presentation	Genuine	—	FNMR
— Out of consideration.				

NOTE 2 The last column expresses decision and relevant error rates.

Table 4 — Relation among error rates, presentation type, and attack classification for full system of biometric identification

System	Presentation type (Input)	Decision (Output)	
		Candidate	Not candidate
Positive identification	Attack	IAPIR	—
	Bona fide	FPIR	—
Negative identification	Attack	—	CAPNIR
	Bona fide	—	FNIR
— Out of consideration.			

7.3 Minimum test sizes and maximum error rates

The test size requirements for PAD testing depend on the magnitude of the error rates to be measured and the acceptable error bounds for the test results. As error rates and acceptable error bounds reduce, statistical considerations require that the test size increases.

For PAD testing, various PAIs representing PAI species and attack types are subject to testing and the results shall be reported for each PAI species and attack type. The test size shall be assessed for each PAI species and attack type.

It is the purpose of functional testing to assess that the PAD is working properly on the TOE.

Thus, all of the standard PAIs or non-standard PAIs do not have be used in functional testing. The evaluator should investigate other possible PAIs during AVA. The minimum number of PAI species, minimum test sizes and maximum error rates for functional testing may be defined either in the standard PAI species or in the evaluation guidance of the considered protection profile. If any recommendation from the certification body is given, the evaluator should consider them to determine the adequate test size per PAI species. If they are not defined, the evaluator shall use at least 10 different samples for each PAI species considered. The minimum number of PAI species, minimum test sizes, and maximum error rates for functional testing shall be agreed between the developer and the evaluator. The minimum test size for each PAI species should be 10. The maximum error rate (APCER) for each PAI species should not be greater than 0,1.

The evaluator should also consider recommendations from other international standards or non-international standards for specific use cases. For instance, in the case of a mobile biometric system, the evaluator should use as a baseline the recommendations given in ISO/IEC 30107-4 for the number of different PAI species and test size.

8 Supplementary activities to ISO/IEC 18045 on vulnerability assessment (AVA)

8.1 Penetration testing using PAI variations

In contrast to the functional testing, the evaluator should consider specific aspects of the TOE in the context of penetration testing. The evaluator shall use information obtained from the evaluation of other assurance classes such as ADV to find potential weaknesses in design or implementation of the TOE. With the results of the analyses, the evaluator shall identify attack types that are potentially able to circumvent the PAD mechanism of the TOE. The evaluator shall look for materials, material mixtures, and techniques that can be used to create PAIs that can defeat the PAD mechanisms of the TOE. The evaluator shall try candidate PAIs that are relevant to the specified level of attack potential for the TOE looking for presentation misclassifications. If a misclassification occurs, the evaluator shall record all relevant details of the PAI and the number of previous correct classifications for the PAI prior to the misclassification occurring. Trials using the same PAI shall continue looking until further misclassifications are found or the evaluator is satisfied that misclassification occurrences are not readily repeatable. No rigid rules can be given on how much time should be spent on a typical evaluation by a competent evaluator. However, as a guidance, the time spent on this activity for AVA_VAN.1 should be around 1 week, while it should be around 2 months for AVA_VAN.5.

A further source of information on relevant attack types that are created for penetration testing is the functional testing. Functional testing can reveal that particular PAIs or attack types result in PAD error rates that are higher than normal for the TOE. These PAIs/attack types may be candidates for further exploration as part of penetration testing. Even if functional testing does not reveal that particular PAIs or attack types result in PAD error rates that are higher than normal for the TOE, there may be different/variant PAIs/attack types that can circumvent the PAD mechanism of the TOE in the penetration testing stage of the evaluation.

Penetration testing in vulnerability analysis has a creative aspect. The effectiveness of a presentation attack depends on the preparation of the PAIs and their presentation. In the case of fingerprint PAIs, the material used affects the success of an attack as do presentation details such as the temperature and thickness of the PAI and the lubrication of its surface with water or oil. For modalities such as face, iris and voice, other influencing factors can include sample rate, video resolution, frame rate, colour space and physical size used in making PAIs. The evaluators should build and maintain the requisite level of preparation and presentation skills through a combination of the monitoring of public domain and other information on presentation attacks against biometric systems and practical training and experiment.

The evaluator shall determine the approach to penetration testing, investigate any potential vulnerabilities that have been identified for the TOE, and acquire or prepare suitable PAIs. During penetration testing, the evaluator shall present all the prepared PAIs to the TOE multiple times using

suitable variations of presentation. If no PAI is found that is able to circumvent the PAD subsystem, the evaluator may conclude that the TOE is resistant to these PAIs.

If a TOE fails to detect a PAI presented during vulnerability assessment, then the TOE is shown to be vulnerable to the PAI/presentation and by implication to other PAI/presentations. The evaluator should seek to reproduce the vulnerability to be able to estimate the difficulty of reproducing it. Practical constraints such as time and variability probably mean that reproducibility can only be estimated on a fairly coarse scale of difficulty (e.g. easy, moderately difficult, very difficult). The level of difficulty of reproducing the vulnerability is a factor in determining the risk involved in using the TOE in an application scenario and in calculating the attack potential. The APCER for a PAI species in the functional testing can be used to inform the penetration testing, for example to highlight PAI species that the TOE can be vulnerable to for further investigation.

Note that some attack scenarios may not need to be covered by penetration testing if the required attack potential of the attack scenario is higher than specified by the AVA_VAN component of the TOE. The attack potential for an attack using a PAI against the TOE PAD mechanism shall be calculated according to the guidance in ISO/IEC 19989-1:2020, Annex D. Examples are provided in Annex A.

ISO/IEC 19989-1:2020, C.1, gives information on other potential TOE vulnerabilities and guidance on penetration testing where applicable to a particular TOE.

8.2 Potential vulnerabilities

The vulnerabilities that the evaluator shall at least take into account are described in ISO/IEC 19989-1:2020, 5.1. Additionally, the evaluator should consider the combination of those vulnerabilities with other IT-related vulnerabilities.

8.3 Rating of vulnerabilities and TOE resistance

The rating shall be done according to ISO/IEC 19989-1:2020, F.1.5, as well as the consideration of the attack potential (see ISO/IEC 19989-1:2020, F.1.2). Examples related to PAD vulnerabilities are provided in Annex A.

Annex A
(informative)

Examples of calculations of attack potential

A.1 General

This annex provides several examples that include various systems that can be evaluated (access control device for a building, an office, etc., access control to a personal device, etc.) and the "classical" attacks that can be applied. Refer to ISO/IEC 19989-1:2020, D.1.2 and ISO/IEC 18045:2008, B.4.

A.2 Example 1 — Simple system without presentation attack detection

Two examples are here rated, 2D face recognition and fingerprint-based systems, unattended and without any restriction to access the TOE. The difference in factors is only access to biometric characteristics.

The following is considered.

— Elapsed time: 1 day is enough to define the method to build an attack type (identification) and to generate a PAI targeting a dedicated person (exploitation). For 2D images, a simple print of a picture can be enough, for fingerprints a moulding with easy to get material (glue, silicon, latex, and so forth) is efficient.

— Expertise: A lot of publications explain how to perform. No specific expertise is required (layperson value is enough).

NOTE The term "layperson" is used for gender neutrality.

— Knowledge of the TOE: No specific knowledge of the TOE is required.

— Window of opportunity (access to the TOE): It does not make any problem to access to the TOE both in identification (easy to buy without control) or in exploitation (a fingerprint PAI is easy to present: for example by "gluing" the PAI to the real finger, for 2D face, a picture is presented to the camera).

— Window of opportunity (access to biometric characteristics): The level is Immediate for 2D face and Easy for fingerprint.

— Equipment: There is no speciffic requirement on equipment.

Table A.1 — Calculation of attack potential for example 1 (2D face)

Elapsed time		Expertise		Knowledge of TOE		Window of opportunity				Equipment		Total	
						Access to TOE		Access to biometric characteristics				0	
Id	Exp	Id	Exp	Id	Exp	Id	Exp	Id	Exp	Id	Exp	Id	Exp
0	0	0	0	0	—	0	0	—	0	0	0	0	0

Table A.2 — Calculation of attack potential for example 1 (Fingerprint)

Elapsed time		Expertise		Knowledge of TOE		Window of opportunity				Equipment		Total	
						Access to TOE		Access to biometric characteristics				2	
Id	Exp	Id	Exp	Id	Exp	Id	Exp	Id	Exp	Id	Exp	Id	Exp
0	0	0	0	0	—	0	0	—	2	0	0	0	2

As shown in Table A.1 and Table A.2, the attack potential for the attack is basic.

The system fails any level of evaluation assuming that the described attack can be performed successfully.

A.3 Example 2 — Fingerprints with presentation attack detection

The system is typically an access control system in an open environment. Consecutive presentations are possible but "strange" behaviour of the user would be detected.

The system includes PAD implying to find the right material for making the attack type (glycerine, gelatin, for example) and the application to a real finger is not immediate (thin film, leaving part of the skin in contact with the capture device, a print with specific ink directly on a real finger, etc.).

The following is considered.

— Elapsed time: Finding the right material for the attack type and how to present it to the system is not evident and requires consecutive presentations. 2 weeks for identification is realistic for an example. Once defined, producing the PAI for a dedicated person and applying with the predefined method to the real TOE is immediate (1 day for exploitation).

— Expertise: A lot of publications explain how to perform. However, the attacker has to understand (and even to find) what is the principle of the PAD, and to derive a specific strategy both for creating the PAI and to apply it. A proficient level for identification is realistic, for exploitation a layperson is enough (following a script).

— Knowledge of the TOE: It is assumed that no specific knowledge is required. The existence of PAD is probably advertised (either by the developer or the user). With some time, the attacker (proficient level, so knowing what is offered by industrial systems) will probably find the method this detection is based on.

— Window of opportunity (access to the TOE): Being a security system, it is assumed that it is not possible to simply buy the system without any control, but that its distribution is controlled (for example by requiring an identification of the buyer and potentially to sign a non-disclosure agreement). Moderate level is adapted for the identification phase and for the exploitation phase (detection of a strange behaviour).

— Window of opportunity (access to biometric characteristics): The level is easy.

— Equipment: There is no specific requirement on equipment.

Table A.3 — Calculation of attack potential for example 2

Elapsed time		Expertise		Knowledge of TOE		Window of opportunity				Equipment		Total	
						Access to TOE		Access to biometric characteristics				12	
Id	Exp	Id	Exp	Id	Exp	Id	Exp	Id	Exp	Id	Exp	Id	Exp
2	0	0	2	0	—	2	4	—	2	0	0	4	8