INTERNATIONAL STANDARD

ISO/IEC 19989-1

First edition
2020-09

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

Part 1: **Framework**

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

Partie 1: Cadre

Reference number
ISO/IEC 19989-1:2020(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

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.

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) or the IEC list of patent declarations received (see http://patents.iec.ch).

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 counter 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 standard 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 the ISO/IEC 19989 series.

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 components together with supplementary activities related to these requirements. The extensions to the requirements and supplementary 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 consists of the introduction of the general framework for the security evaluation of biometric systems, including extended security functional components, and supplementary methodology and evaluation activities for the evaluator. The detailed recommendations are developed for biometric recognition aspects in ISO/IEC 19989-2 and for presentation attack detection aspects in ISO/IEC 19989-3.

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 1: Framework

1 Scope

For security evaluation of biometric recognition performance and presentation attack detection for biometric verification systems and biometric identification systemsthis document specifies:

- extended security functional components to SFR Classes in ISO/IEC 15408-2;
- supplementary activities to methodology specified in ISO/IEC 18045 for SAR Classes of ISO/IEC 15408-3.

This document introduces the general framework for the security evaluation of biometric systems, including extended security functional components, and supplementary activities to methodology, which is additional evaluation activities and guidance/recommendations for an evaluator to handle those activities. The supplementary evaluation activities are developed in this document while the detailed recommendations are developed in ISO/IEC 19989-2 (for biometric recognition aspects) and in ISO/IEC 19989-3 (for presentation attack detection aspects). This document is applicable only to TOEs for single biometric characteristic type. However, the selection of a characteristic from multiple characteristics in SFRs is allowed.

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 2382:2008, *Information technology — Vocabulary*

ISO/IEC 2382-37:2017, *Information technology — Vocabulary— Part 37: Biometrics*

ISO/IEC 15408-1:2009, *Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model*

ISO/IEC 15408-2:2008, *Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional components*

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

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

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 2382:2008, ISO/IEC 2382-37:2017, ISO/IEC 15408-1:2009, ISO/IEC 18045:2008, 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 https://www.iso.org/obp

3.1
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

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

3.2
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

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

3.3
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]

3.4
bona fide presentation classification error rate
BPCER
proportion of bona fide presentations incorrectly classified as presentation attacks in a specific scenario

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

3.5
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]

3.6
penetration testing
testing used in vulnerability analysis for vulnerability assessment, trying to defeat 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.

3.7
presentation attack
presentation to the biometric data capture subsystem with the goal of interfering with the operation of the biometric system

Note 1 to entry: Presentation attack can be implemented through a number of methods, e.g. artefact, mutilations, replay, etc.

Note 2 to entry: Presentation attacks may have a number of goals, e.g. impersonation or not being recognized.

Note 3 to entry: Biometric systems may not be able to differentiate between biometric presentation attacks with the goal of interfering with the systems operation and non-conformant presentations.

[SOURCE: ISO/IEC 30107-1:2016, 3.5]

3.8
presentation attack detection
PAD
automated determination of a presentation attack

Note 1 to entry: PAD cannot infer the subject's intent. In fact it may be impossible to derive that difference from the data capture process or acquired sample.

[SOURCE: ISO/IEC 30107-1:2016, 3.6]

3.9
presentation attack instrument
PAI
biometric characteristic or object used in a presentation attack

Note 1 to entry: The set of PAI includes artefacts but would also include lifeless biometric characteristics (i.e. stemming from dead bodies) or altered biometric characteristics (e.g. altered fingerprints) that are used in an attack.

[SOURCE: ISO/IEC 30107-1:2016, 3.7]

Note 2 to entry: Examples of altered biometric characteristics are mutilation, surgical switching of fingerprints between hands and/or toes (See Table 1 in 5.2 of ISO/IEC 30107-1:2016).

4 Symbols and abbreviated terms

APCER	attack presentation classification error rate
BPCER	bona fide presentation classification error rate
IT	information technology
FAR	false acceptance rate
FAU	SFR class of audit

NOTE The class name is defined in ISO/IEC 15408-2. Here, F of FAU stands for functional requirement, AU for audit. The class name is defined in this way in the ISO/IEC 15408 series. For details, see Annex A.

FMR	false match rate
FNIR	false-negative identification-error rate
FNMR	false non-match rate
FPIR	false-positive identification-error rate
FPT	SFR class of protection of the TSF
	NOTE See NOTE to FAU.
FRR	false rejection rate
FTAR	failure-to-acquire rate
FTER	failure-to-enrol rate
PAD	presentation attack detection
PAI	presentation attack instrument
PP	protection profile
SAR	security assurance requirement
SFR	security functional requirement
ST	security target
TOE	target of evaluation
TSF	TOE security functionality
TSFI	TSF interface

5 General remarks

In addition to the requirements and recommendations provided in Clause 7 and Clause 8, those in ISO/IEC 15408-2 shall be applied.

In addition to the requirements and recommendations provided in Clause 9 to Clause 15, those in ISO/IEC 15408-3 and ISO/IEC 18045 shall be applied.

Annex D provides background information on supplementary activities for PAD evaluation.

The definition of authentication can be found in ISO/IEC 2382.

The definitions of biometric (adjective), biometric capture, assurance, biometric capture device, biometric characteristic, biometric concealer, biometric enrolee, biometric enrolment, biometric enrolment database, biometric feature, biometric identification, biometric impostor, biometric presentation, biometric recognition, biometrics, biometric reference, biometric sample, biometric system, biometric verification, comparison, enrol, failure-to-acquire rate, failure-to-enrol rate, alse match rate, false-negative identification-error rate, false non-match rate, false-positive identification-error rate, identify, match (noun) and threshold (noun) can be found 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 "impostor" is sometimes used instead of "biometric impostor".

The definitions of administrator, assignment, assurance, attack potential, class, component, confirm, delivery, describe, determine, developer, development, element, ensure, evaluation, extension, family, guidance documentation, identity, interaction, interface, life-cycle, object, operation ⟨on a component of ISO/IEC 15408⟩, operation, operational environment, potential vulnerability, Protection Profile, Protection Profile evaluation, security requirement, Security Target, ST evaluation, subject, target of evaluation, TOE security functionality, TSF data, TSF interface, TSF self-protection, verify and vulnerability can be found in ISO/IEC 15408-1.

NOTE 4 The second "operation" is related to the AGD class.

The definitions of action, activity, check, examine, methodology, report, scheme, sub-activity and work unit can be found in ISO/IEC 18045.

6 Vulnerabilities in biometric systems and security evaluation

6.1 Categorization of common vulnerabilities of biometric systems

In ISO/IEC 19792:2009, 8.3, common vulnerabilities of biometric systems are categorized into the following ten factors:

a) performance limitations;

b) artefact of biometric characteristics;

c) modification of biometric characteristics;

d) difficulty of concealing biometric characteristics;

e) similarity due to blood relationship;

f) special biometric characteristics;

g) synthesized wolf biometric samples;

h) hostile environment;

i) procedural vulnerabilities around the enrolment process; and

j) leakage and alteration of biometric data.

NOTE 1 All of the factors listed above are not vulnerabilities of biometric systems but each is related to them. In this document, the vulnerabilities of the factors or those related to factors, and their relations to security evaluation are considered.

Figure 1 shows the relationship between the vulnerability factors described in ISO/IEC 19792 and the types of evaluation described in this document.

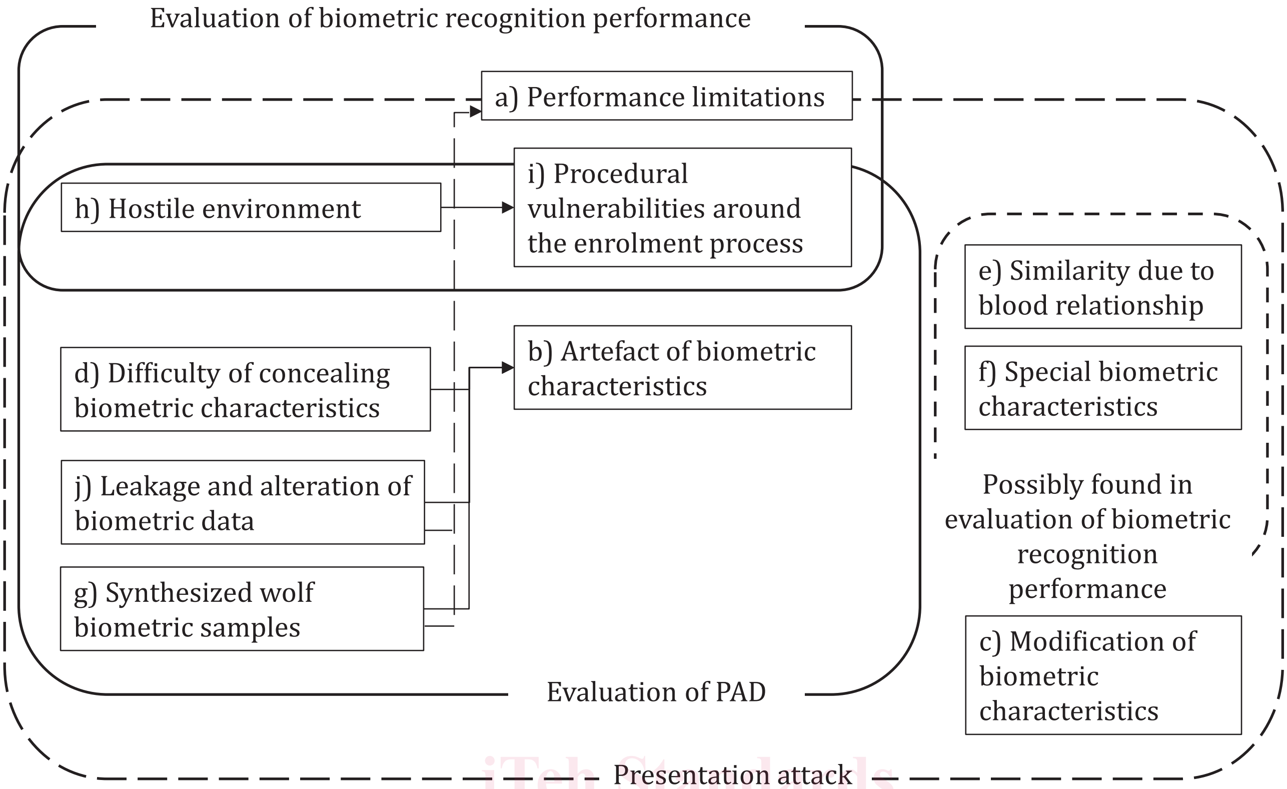
Evaluation of biometric recognition performance
a) Performance limitations
h) Hostile environment
i) Procedural vulnerabilities around the enrolment process
e) Similarity due to blood relationship
f) Special biometric characteristics
d) Difficulty of concealing biometric characteristics
b) Artefact of biometric characteristics
j) Leakage and alteration of biometric data
Possibly found in evaluation of biometric recognition performance
g) Synthesized wolf biometric samples
c) Modification of biometric characteristics
Evaluation of PAD
Presentation attack

Figure 1 — The relation of vulnerability factors in biometric systems

Factor j) is important as related to the protection of TSF-data/used data (see ISO/IEC 19792). In this document, however, factor j) is considered only from the standpoint of its exploitation by attackers to facilitate the construction of PAIs or mounting attacks related to biometric recognition performance. The evaluation of measures to protect biometric data from leakage or alteration is not addressed here.

Factor a), inherent in all biometric systems, can lead to false acceptances and false rejections, and is addressed in the biometric recognition performance evaluation. However, it can be also considered in relation to the zero-effort attack (presentation from impostor attempts under the policy of the intended use following the TOE guidance documentation). Thus, the biometric recognition performance evaluation and the PAD evaluation interrelate to each other. This factor is relevant to enrolment, verification, and identification.

Other factors are relevant to presentation attacks. However, factors e) and f) are out of scope for a PAD evaluation. Factor f) relates to individuals who have unusual natural biometric characteristics that make them more than usually liable to generate an apparent match against those of other people. However, such individuals are likely to be very difficult to find for the purpose of testing during an evaluation. They can be accidentally found as the result of the evaluation of biometric recognition performance. For factor e), it is difficult to collect such samples for the security evaluation. Outlier subjects giving rise to abnormally high biometric recognition performance can be encountered during biometric recognition performance testing. This can reveal a potential vulnerability in the TOE and relevant information should be used to inform the AVA evaluation activity.

Factor c) may be seen as a means of presentation attack that would exploit recognition weaknesses such as those revealed with a) and f) but thus to be considered in the vulnerability analysis phase. However, it requires extra elements beyond the scope of the objective evaluation. For example, surgery to embed the biometric characteristic of another person requires a sacrifice by the test subject and mimicry requires special skills to be developed by them.

Therefore, factors b), d), g), h), and i) are the factors to be evaluated in ISO/IEC 15408 evaluation for PAD. Factor i) needs to be considered only in enrolment. Factors b), g), and h) are relevant to