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.