INTERNATIONAL STANDARD

ISO/IEC 19792

First edition
2009-08-01

Information technology — Security techniques — Security evaluation of biometrics

Technologies de l'information — Techniques de sécurité — Cadre de la sécurité pour l'évaluation et le test de la technologie biometrique

Reference number
ISO/IEC 19792:2009(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web 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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

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.

ISO/IEC 19792 was prepared by Technical Committee ISO/TC JTC1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

Information technology — Security techniques — Security evaluation of biometrics

1 Scope

This International Standard specifies the subjects to be addressed during a security evaluation of a biometric system.

It covers the biometric-specific aspects and principles to be considered during the security evaluation of a biometric system. It does not address the non-biometric aspects which might form part of the overall security evaluation of a system using biometric technology (e.g. requirements on databases or communication channels).

This International Standard does not aim to define any concrete methodology for the security evaluation of biometric systems but instead focuses on the principal requirements. As such, the requirements in this International Standard are independent of any evaluation or certification scheme and will need to be incorporated into and adapted before being used in the context of a concrete scheme.

This International Standard defines various areas that are important to be considered during a security evaluation of a biometric system. These areas are represented by the following clauses of this International Standard:

— Clauses 4 and 5 of this International Standard give an overview of all terms, definitions and acronyms used,

— Clause 6 introduces the overall concept for a security evaluation of a biometric system,

— Clause 7 describes statistical aspects of security-relevant error rates,

— Clause 8 deals with the vulnerability assessment of biometric systems and

— Clause 9 describes the evaluation of privacy aspects.

This International Standard is relevant to both evaluator and developer communities.

— It specifies requirements for evaluators and provides guidance on performing a security evaluation of a biometric system.

— It serves to inform developers of the requirements for biometric security evaluations to help them prepare for security evaluations.

Although this International Standard is independent of any specific evaluation scheme it could serve as a framework for the development of concrete evaluation and testing methodologies to integrate the requirements for biometric evaluations into existing evaluation and certification schemes.

This International Standard refers to and utilizes other biometric standards, notably those for biometric performance testing and reporting from ISO/JTC1 SC 37. These standards have been adapted as necessary for the specific requirements of biometric security evaluation.

2 Conformance

To conform to this International Standard, a security evaluation of a biometric system shall be planned, executed and reported in accordance with the normative requirements contained herein.

This International Standard describes the specific aspects of a security evaluation of a biometric system in terms of

— statistical error rates (see Clause 7),

— biometric-specific vulnerabilities (see Clause 8), and

— privacy (see Clause 9)

As some evaluation schemes that adopt this International Standard may not address all of the aforementioned aspects it shall further be possible to claim conformance to parts of this International Standard. In this case a security evaluation of a biometric system shall be planned, executed and reported in accordance with a subset of the normative requirements of this International Standard. In this case the requirements that are addressed shall be clearly identified.

Note that conformance to this International Standard is limited to the adoption of the biometric evaluation methodology described and adherence to the specified normative requirements. Conformance does not include scheme related issues such as action to be taken in the event that a system under evaluation fails to meet security relevant evaluation criteria or targets. The overarching scheme is responsible for specifying this action, which could include, for example:

— outright evaluation failure,

— restatement of evaluation criteria or targets to match achieved results, or

— development of a system under evaluation to meet specified evaluation criteria or targets.

3 Normative references

The following referenced documents are indispensable for the application 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 19795-1:2006, *Biometric performance testing and reporting — Part 1: Principles and framework*

4 Terms and definitions

4.1 General

4.1.1
assurance level
amount of assurance obtained according to the specific scale used by the assurance method

NOTE Definition from [1].

4.1.2
attacker
person seeking to exploit potential vulnerabilities of a biometric system

4.1.3
biometric characteristic
biological and behavioural characteristic of an individual that can be detected and from which distinguishing, repeatable biometric features can be extracted for the purpose of automated recognition of individuals

NOTE 1 Definition from [2].

NOTE 2 Biological and behavioural characteristics are physical properties of body parts, physiological and behavioural processes created by the body and combinations of any of these.

NOTE 3 Distinguishing does not necessarily imply individualization.

EXAMPLE Examples of biometric characteristics are: Galton ridge structure, face topography, facial skin texture, hand topography, finger topography, iris structure, vein structure of the hand, ridge structure of the palm or retinal pattern.

4.1.4
biometric product
biometric component, system or application acting as the scope of an evaluation

4.1.5
biometrics
automated recognition of individuals based on their behavioural and biological characteristics

NOTE Definition from [2].

4.1.6
evaluator
person or party responsible for performing a security evaluation of a biometric product

4.1.7
evaluation
assessment of a deliverable against defined criteria

NOTE 1 Definition from [1].

NOTE 2 In this context, a deliverable is a biometric system.

4.1.8
lamb
biometric reference that results in higher than normal similarity scores on a particular biometric system when compared to biometric samples or references from other subjects

4.1.9
vendor
party that sells, produces or uses a biometric system and is responsible for providing the biometric system and all necessary evidence for evaluation

NOTE In cases where a vendor decides to delegate certain tasks to another party (e.g. to a third party testing laboratory), this party shall be seen as a vendor as well.

4.1.10
user
person interacting with a biometric system

4.1.11
wolf
biometric sample that results in higher than normal similarity scores on a particular biometric system when compared to biometric references of enrolees

4.2 Biometric systems

4.2.1
attempt
submission of one (or a sequence of) biometric samples to the system

NOTE An attempt results in an enrolment template, a matching score (or scores), or possibly a failure-to-acquire.

4.2.2
biometric data
biometric sample at any stage of processing, biometric reference, biometric feature or biometric property

NOTE Definition from [2].

4.2.3
biometric feature
numbers or labels extracted from biometric samples and used for comparison

NOTE 1 Biometric features are the output of a completed biometric feature extraction.

NOTE 2 The use of this term should be consistent with its use by the pattern recognition and mathematics communities.

NOTE 3 A biometric feature set can also be considered a processed biometric sample.

4.2.4
biometric model
stored function (dependent on the biometric data subject) generated from a biometric feature(s)

NOTE 1 Definition from [2].

NOTE 2 Comparison applies the function to the biometric features of a recognition biometric sample to give a comparison score.

NOTE 3 The function may be determined through training.

NOTE 4 A biometric model may involve intermediate processing similar to biometric feature extraction.

EXAMPLE Examples for the stored function could be a Hidden Markov Model, Gaussian Mixture Model or an Artificial Neural Network.

4.2.5
biometric property
descriptive attributes of the biometric data subject estimated or derived from the biometric sample by automated means

NOTE Definition from [2].

EXAMPLE Fingerprints can be classified by the biometric properties of ridge-flow, i.e. arch, whorl, and loop types; In the case of facial recognition, this could be estimates of age or gender.

4.2.6
biometric reference
one or more stored biometric samples, biometric templates or biometric models attributed to a biometric data subject and used for comparison

NOTE 1 Definition from [2].

NOTE 2 A biometric reference may be created with implicit or explicit use of auxiliary data, such as Universal Background Models.

EXAMPLE Face image on a passport; Fingerprint minutiae template on a National ID card; Gaussian Mixture Model, for speaker recognition, in a database.

4.2.7
biometric sample
analog or digital representation of biometric characteristics prior to biometric feature extraction and obtained from a biometric capture device or biometric capture subsystem

NOTE 1 Definition from [2].

NOTE 2 A biometric capture device is a biometric capture subsystem with a single component.

4.2.8
biometric template
set of stored biometric features comparable directly to biometric features of a recognition biometric sample

NOTE 1 Definition from [2].

NOTE 2 A biometric reference consisting of an image, or other captured biometric sample, in its original, enhanced or compressed form, is not a biometric template.

NOTE 3 The biometric features are not considered to be a biometric template unless they are stored for reference.

4.2.9
enrolment data record
record created upon enrolment, associated with an individual and including biometric reference(s) and typically non-biometric data

NOTE Definition from [2].

4.2.10
transaction
sequence of attempts on the part of a user for the purposes of an enrolment, biometric verification or biometric identification

NOTE There are three types of transaction: an enrolment sequence, resulting in an enrolment or a failure-to-enrol; a verification sequence, resulting in a verification decision; or an identification sequence, resulting in an identification decision.

4.3 Biometric processes

4.3.1
authentication
provision of assurance of the claimed identity of an entity

NOTE Definition from [1].

4.3.2
biometric application decision
conclusion based on the application decision policy after consideration of one or more comparison decisions, comparison scores and possibly other non-biometric data

NOTE 1 Definition from [2].

NOTE 2 Biometric application decisions can be made on the basis of complex policies, allowing for variable numbers of positive comparison decisions.

NOTE 3 A biometric verification application could allow a positive biometric application decision even if there are one or more non-matches against enrolled biometric references.

EXAMPLE A biometric application decision could be “accept claim”.

4.3.3
biometric recognition
recognition using a biometric product

NOTE A biometric recognition can either be realized as a biometric verification or as a biometric identification process.

4.3.4
comparison score
numerical value (or set of values) resulting from a comparison

NOTE Definition from [2].

4.3.5
de-enrolment
deletion of the biometric reference from storage and if necessary, associated data in connection with the end-user's identity from the biometric system

4.3.6
decision policy
collection of parameters, rules and values used to determine the acceptance or rejection of the biometric recognition of the subject

4.3.7
enrol
create and store an enrolment data record for a biometric capture subject in accordance with an enrolment policy

NOTE Definition from [2].

4.3.8
enrolment
action of enrolling or being enrolled

NOTE Definition from [2].

4.3.9
biometric identification
biometric system function that performs a one-to-many search to obtain a candidate list

NOTE Definition from [2].

4.3.10
comparison decision
determination of whether the recognition biometric sample(s) and biometric reference(s) have the same biometric source, based on a comparison score(s), a decision policy(ies) including a threshold, and possibly other inputs

NOTE 1 Definition from [2].

NOTE 2 A match is a positive comparison decision.

NOTE 3 A non-match is a negative comparison decision.

NOTE 4 A decision of “undetermined” can sometimes be given.

4.3.11
threshold
boundary value of the comparison score used by the comparison application to automatically generate the matching decision

4.3.12
biometric verification
biometric product function that performs a one-to-one comparison

NOTE Adapted from [2].

4.4 Error rates

NOTE Definitions 4.4.1 to 4.4.9 and 4.4.11 are from ISO/IEC 19795-1:2006.

4.4.1
active impostor attempt
attempt in which an individual tries to match the stored template of a different individual by presenting a simulated or reproduced biometric sample, or by intentionally modifying his/her own biometric characteristics

4.4.2
failure-to-enrol rate
FTE
proportion of the population for whom the system fails to complete the enrolment process

NOTE The observed failure-to-enrol rate is measured on test crew enrolments. The predicted/expected failure-to-enrol-rate will apply to the entire target population.

4.4.3
false non-match rate
FNMR
proportion of genuine attempt samples falsely declared not to match the template of the same characteristic from the same user supplying the sample

NOTE The measured/observed false non-match rate is distinct from the predicted/expected false non-match rate (the former may be used to estimate the latter).

4.4.4
false match rate
FMR
proportion of zero-effort impostor attempt samples falsely declared to match the compared non-self template

NOTE The measured/observed false match rate is distinct from the predicted/expected false match rate (the former may be used to estimate the latter).

4.4.5
false reject rate
FRR
proportion of verification transactions with truthful claims of identity that are incorrectly denied

4.4.6
false accept rate
FAR
proportion of verification transactions with wrongful claims of identity that are incorrectly confirmed

4.4.7
identification rank
smallest value k for which a user's correct identifier is in the top k identifiers returned by an identification system

NOTE The Identification rank is dependent on the size of the enrolment database, and should be quoted “rank k out of n”.

4.4.8
pre-selection algorithm
algorithm to reduce the number of templates that need to be matched in an identification search of the enrolment database

4.4.9
pre-selection error
⟨pre-selection algorithm⟩ error that occurs when the corresponding enrolment template is not in the preselected subset of candidates when a sample from the same biometric characteristic on the same user is given

NOTE In pre-selection that is based on building partitions/classes of users, pre-selection errors happen when the enrolment template and a subsequent sample from the same biometric characteristic on the same user are placed in different partitions.

4.4.10
test crew
set of test subjects gathered for an evaluation

NOTE Definition from [1].

4.4.11
zero-effort impostor attempt
attempt in which an individual submits his/her own biometric characteristics as if he/she were attempting successful verification against his/her own template, but the comparison is made against the template of another user

4.5 Statistical

4.5.1
confidence interval

lower estimate L and an upper estimate U for a parameter x such that the probability of the true value of x being between L and U is the stated value (e.g. 95 %)

[ISO/IEC 19795-1:2006, definition 4.8.2]

NOTE A confidence interval is always associated with a corresponding stated value of probability. In this International Standard the stated value of probability is termed "confidence value"

4.5.2
confidence value
stated value of probability corresponding to a specified confidence interval

5 Abbreviated terms

DET	detection error tradeoff (curve)
FAR	false accept rate
FDIS	Final Draft International Standard
FMR	false match rate
FNMR	false non-match rate
FRR	false reject rate
FTE	failure-to-enrol
IS	International Standard

6 Security evaluation

6.1 Overview

This clause further delineates the scope of this International Standard described in Clause 1 and provides a context in which the security evaluation of biometrics is conducted.

Figure A.1 shows the reference architecture of a biometric system used in this International Standard. A biometric system comprises a collection of hardware and software components. It is normally used to implement a biometric application, in which case it operates in an externally provided environment that forms an essential part of the application. The environment comprises not only physical factors such as space, temperature, humidity, illumination, etc., but also all procedural aspects and human users of the system. Users of the system comprise all classes of people who might interact with the system such as operators, administrators, enrolees, impostors etc.

This International Standard is principally directed at the security evaluation of biometric systems themselves rather than complete biometric applications. A biometric application comprises a biometric system and possibly other hardware and software components, together with an operating environment, organisational processes and policies that collectively provide the functionality of the application. These additional elements may have security vulnerabilities of their own or might amplify or mitigate vulnerabilities possessed by the biometric system itself.

Vulnerability assessment should be conducted in an ordered manner that will involve the investigation of individual component vulnerabilities. Evaluators should, however, exercise caution when assessing the results of component vulnerability assessment without considering the interactions that take place with other system components. These interactions can determine whether or not component vulnerabilities can be exploited in practice. Therefore evaluators should always assess vulnerabilities in the context of the overall system functioning and not solely based on assessment of individual component vulnerabilities.

Similarly, a biometric system may display intrinsic vulnerabilities that are realised, aggravated or mitigated by interaction among system components. For example, a biometric comparison algorithm may display anomalous behaviour if presented with out of range biometric data, and this behaviour could give rise to a vulnerability. However, if the component(s) responsible for supplying the biometric data to the comparison algorithm prevents such anomalous data being supplied, there is no resultant vulnerability. Although the methodology in this International Standard could be used to evaluate security factors for components of a biometric system, evaluators should exercise caution when examining individual component vulnerabilities and seek to understand the interactions between components to determine how these may affect the resulting system vulnerabilities. In general the assessment of individual component vulnerabilities may have limited value and be misleading if conducted outside the context of a system evaluation.

This International Standard specifies a methodology for the evaluation of the technical security of biometric systems. It does not seek to address the broader issues of security evaluation of a complete biometric application. Accreditors of biometric applications will therefore need to develop threat/risk models for applications and to assess whether other non-biometric specific vulnerabilities exist in the overall system and what effect any biometric vulnerabilities discovered may have on the overall system security.

6.2 Methodology

This International Standard addresses the aspects of security evaluation that are specific to biometric systems. A biometric system security evaluation will probably also involve the evaluation of IT security aspects. This International Standard does not cover these aspects and evaluators should refer to other IT security evaluation standards and methodologies for the evaluations of non-biometric aspects of a system security evaluation, e.g. Common Criteria ([3]).