INTERNATIONAL STANDARD

ISO/IEC 30107-4

First edition
2020-06

Information technology — Biometric presentation attack detection —

Part 4: Profile for testing of mobile devices

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

Partie 4: Profil pour les essais des dispositifs mobiles

Reference number
ISO/IEC 30107-4:2020(E)

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

Published in Switzerland

Contents

Page

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 37, *Biometrics*.

A list of all parts in the ISO/IEC 30107 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

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

PAD subsystems are commonly integrated into mobile devices[1]. The following characteristics of mobile devices necessitate the development of a profile of ISO/IEC 30107-3 specific to PAD testing[2]:

— Mobile devices often have accelerated product development timelines, such that time and resources for PAD testing may be limited.

— A single type of biometric subsystem is often integrated into a wide range of mobile devices, so results from a single test may be applicable to multiple types of mobile devices.

— Biometric subsystems integrated into mobile devices are typically closed systems, such that performance testing takes place through a full-system evaluation.

This document provides requirements for assessing the performance of PAD mechanisms on mobile devices with local biometric recognition.

Information technology — Biometric presentation attack detection —

Part 4:
Profile for testing of mobile devices

1 Scope

This document is a profile that provides requirements for testing biometric presentation attack detection (PAD) mechanisms on mobile devices with local biometric recognition.

This document lists requirements from ISO/IEC 30107-3 specific to mobile devices. It also establishes new requirements not present in ISO/IEC 30107-3. For each requirement, the profile defines an *Approach in Presentation Attack Detection (PAD) Testing for Mobile Devices*. For some requirements, numerical values or ranges are provided in the form of best practices.

This profile is applicable to mobile devices that operate as closed systems with no access to internal results, including mobile devices with local biometric recognition as well as biometric modules for mobile devices.

Out of the scope of this document are the following:

— mobile devices solely with remote biometric recognition.

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

2 Normative references

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

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

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

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

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

3 Terms, definitions, and abbreviated terms

For the purposes of this document, the terms and definitions given in ISO/IEC 2382-37, ISO/IEC 19795-1, ISO/IEC 30107-1, ISO/IEC 30107-3 and the following 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
mobile device
small, compact, handheld, lightweight, standalone computing device, typically having a display screen with digitizer input and/or a miniature keyboard

Note 1 to entry: Examples include laptops, tablet PCs, wearable information and communication technology (ICT) devices, and smartphones.

3.2
impostor attack presentation accept rate
IAPAR
<full-system evaluation of a verification system> proportion of impostor attack presentations using the same presentation attack instrument (PAI) species that result in accept

3.3
$IAPAR_{AP}$
impostor attack presentation accept rate (IAPAR) (3.2) of the most successful PAI species with attack potential (AP)

3.4
PAI presenter
set of one or more individuals or mechanisms presenting the PAI to the biometric system

3.5
PAI source
set of one or more individuals or mechanisms from which biometric samples are obtained for use in a PAI, realized in a PAI series

3.6
PAI creator
set of one or more individuals or mechanisms responsible for the conception, formulation, design, and realization of a PAI species

4 Conformance

To conform to this document, a PAD evaluation on mobile devices shall be planned, executed, and reported in accordance with all requirements set forth in Table 1.

5 Profile for PAD testing of mobile devices

The following table provides a profile for PAD testing of mobile devices. Entries in italics represent new requirements not present in ISO/IEC 30107-3. Requirements are numbered as (1), (2), and so forth for ease of reference.

Table 1 — Profile for PAD testing of mobile devices

ISO/IEC 30107-3 Clause	Requirement	Approach in Presentation Attack Detection (PAD) testing of mobile devices
6	(1) Evaluations of PAD mechanisms and resulting reports shall specify the type of presentation attacker — biometric impostor or biometric concealer — considered in an evaluation.	Biometric impostor.
6	(2) Evaluations of PAD mechanisms and resulting reports shall describe the type of evaluation conducted as well as the attack types to be tested.	The evaluator shall specify one of the following: — Application-focused evaluations of PAD mechanisms in which the set/range of attack types is selected to be appropriate to the application, such as those discussed in ISO/IEC 30107-3: 2017, Clause 11; — Product-specific evaluations of PAD mechanisms, used to test a supplier's claim of performance against a specific category of attack types.
7.1	(3) PAD evaluations and resulting reports shall fully describe the IUT, including all configurations and settings as well as the amount of information available to the evaluator about PAD mechanisms in place.	The evaluator shall provide narrative, to include the following: — Mobile device model, operating system (OS), and OS version; — Position of sensor (e.g. front, back, side), to include position relative to device's screen(s); — If applicable, manner of test subject interaction with the biometric sensor (e.g. touch left index finger, swipe right or left thumb, look at front-facing camera, speak a passphrase).
7.1	(4) Evaluations of PAD mechanisms and resulting reports shall specify the applicable evaluation level, whether PAD subsystem, data capture subsystem, or full system.	Full system
7.2	(5) Evaluations of PAD mechanisms shall cover a defined variety of attack types by utilizing a representative set of presentation attack instruments and a representative set of bona fide *test* subjects.	The evaluator shall determine a suitable range of presentation attack instruments (PAIs) and bona fide test subject composition.
7.2	(6) The evaluator shall define the parameters of the attack presentation to fully characterize the range of *PAI presenter* interactions with the IUT, to include the temporal boundaries of the presentation.	The evaluator shall provide basis and narrative.
7.2	(7) In an evaluation of PAD mechanisms, the evaluator shall (a) define bona fide presentations and representative *test* subjects for the target application and population; and (b) provide a rationale for these definitions.	The evaluator shall provide basis and narrative.

Table 1 *(continued)*

ISO/IEC 30107-3 Clause	Requirement	Approach in Presentation Attack Detection (PAD) testing of mobile devices
10.2	(8) Evaluations of PAD mechanisms and resulting reports shall describe how artefacts were created and prepared, to *include*: — creation and preparation processes; — effort required to create and prepare artefacts (e.g. technical know-how, creation time, difficulty of collecting artefact materials, creation instruments, and preparation instruments); — ability to consistently create and prepare artefacts with intended properties; — customization of artefacts for specific *PAI presenters;* — customization of artefacts for specific systems; — sourcing of biometric characteristics; — availability of public information on creation and preparation process; and — changes in artefact creation or preparation processes over the course of the evaluation.	The evaluator shall provide basis and narrative for each bullet point.
10.3	(9) Evaluations of PAD mechanisms and resulting reports shall describe how artefacts were used in the evaluation: — level of *PAI presenter* training and habituation; — artefact durability, including the number of presentations associated with each artefact; and — level of scrutiny or oversight applied during artefact usage.	The evaluator shall provide basis and narrative for each bullet point. Assumption: No scrutiny or oversight is applied during artefact usage.
11.1	(10) Evaluations of PAD mechanisms and resulting reports shall describe whether evaluation design considered enrolment, identification, and/or verification processes.	One or more of the following: enrolment, verification, positive identification.

Table 1 *(continued)*

ISO/IEC 30107-3 Clause	Requirement	Approach in Presentation Attack Detection (PAD) testing of mobile devices
11.2	(11) Evaluations of PAD mechanisms and resulting reports that apply to enrolment processes shall describe the following: — use of enrolment specific quality thresholds or presentation policy; — parameters of the enrolment transaction, including number and duration of presentations; — level of operator oversight present in the process; — manner in which operator functions were applied or emulated in the evaluation; and — *whether the IUT checks sample quality and provides feedback to the test subject (e.g. "finger too wet", "move to a quieter room").*	The evaluator shall provide basis and narrative for each bullet point. Assumptions for enrolment processes include the following: — enrolment parameters are native to the device and are not changeable or exposed to the evaluator; — no operator oversight is present; and — no operator functions are applied or emulated in the evaluation.
11.3	(12) Evaluations of PAD mechanisms and resulting reports that apply to verification processes shall describe the following: — use of quality thresholds and presentation policy; — parameters of the verification transaction, including the number and duration of presentations; — level of operator oversight present in the process; — manner in which operator functions were applied or emulated in the evaluation; — *whether the IUT checks sample quality and provides feedback to the test subject (e.g. "finger too wet");* — *policy after failing all attempts, e.g. asking for a PIN, a password, or waiting for 30 seconds before attempting again;* — *Whether the IUT provides feedback after a failed attempt; and* — *If the IUT provides feedback, a list of the feedback messages.*	The evaluator shall provide basis and narrative for each bullet. Assumptions for verification processes include the following: — verification parameters are native to the device and not changeable or exposed to the evaluator; — no operator oversight is present in the process; and — no operator functions are applied or emulated in the evaluation. Thorough and accurate documentation of transaction policies, attempt limits, and user feedback is particularly important when considering mobile devices. Policies that lead to user revocation and/or device locking after a number of failed attempts can make an evaluation impractical. Special evaluation settings allowing sequences of multiple failed transactions can be requested of the device manufacturer to allow an efficient evaluation. NOTE The behaviour of the IUT after failed transactions can also influence attack approaches. Feedback provided by the IUT can influence IAPAR, as PAI presenters can improve their attack presentations by adapting the artefact creation process in response to feedback.

Table 1 *(continued)*

<table>
<tr><th>ISO/IEC 30107-3 Clause</th><th>Requirement</th><th>Approach in Presentation Attack Detection (PAD) testing of mobile devices</th></tr>
<tr><td></td><td></td><td>EXAMPLE 1 Feedback provided by the mobile device can include the following:<table><tr><th>Modality</th><th>Feedback message from mobile device</th></tr><tr><td>Fingerprint</td><td>“Finger too wet”</td></tr><tr><td>Fingerprint</td><td>“Make sure that your finger covers the entire Home key”</td></tr><tr><td>Face</td><td>“Look at the camera”</td></tr><tr><td>Voice</td><td>“Move to quieter place”</td></tr></table></td></tr>
<tr><td>13.1</td><td>(13) Evaluations of PAD mechanisms shall report the following:
— (14) number of presentation attack instruments used in the evaluation;
— (15) number of PAI species used in the evaluation;
— (16) number of PAI series used in the evaluation;
— (17) number of individuals involved in the testing, including PAI presenters unable to utilize artefacts and test subjects unable to present non-conformant characteristics; and
— (18) number of PAI sources from which artefact characteristics were derived;</td><td>The evaluator shall provide basis and narrative for each bullet point.
The evaluator shall document this figure based on number of IUTs, PAI sources, PAI presenters, PAI species and PAI series.
Best practice is to use a minimum of three PAI species.
PAD testing designed to assess susceptibility to a broader range of attacks would require that more PAI species be used.
EXAMPLE The FIDO Biometrics Requirements methodology[3] specifies use of 10 PAI species.
Best practice is to use a minimum of 10 PAI series per applicable PAI species.
NOTE Certain evaluations might need to take place with fewer than 10 PAI series, such as evaluations utilizing expensive, high-quality masks.
To account for the full range of distinct and potentially overlapping roles in a PAD test, the experimenter shall, in the test report:
— Define the purpose and responsibilities of each role in a PAD test. Roles in a PAD test are as follows:
— test subject (conducts bona fide presentations and non-conformant capture attempts),
— PAI presenter,
— PAI source,
— PAI creator;</td></tr>
</table>

Table 1 *(continued)*

ISO/IEC 30107-3 Clause	Requirement	Approach in Presentation Attack Detection (PAD) testing of mobile devices
		— State whether the role was material to test results and provide a basis for this assertion; — Indicate the number of individuals who occupied each role (e.g. five individuals were PAI sources in the test); — For each role, describe individuals' level of experience with presentation attacks; and — Document occurrences in which individuals occupied multiple roles, e.g. PAI sources were also PAI presenters. Test reports shall describe any use of machines or automated mechanisms as PAI presenters or PAI sources. See Annex A.
	— (19) number of artefacts created per *PAI source* for each *species*;	Best practice is to create a minimum of three PAIs per PAI source for each PAI species. NOTE 1 This is equivalent to the length of a PAI series. NOTE 2 PAD testing not concerned with repeatability of PAIs can allow for fewer PAIs to be created per PAI species and PAI source. EXAMPLE The FIDO Biometrics Requirements methodology specifies use of one PAI per PAI species and test subject.
	— (20) number of tested materials;	The evaluator shall provide basis and narrative.
	— (21) description of output information available from PAD mechanism;	The evaluator shall provide basis and narrative, based on native system operations.
	— (22) ordering of presentations with and without PAI, and whether *PAI presenters* or *test* subjects were reused; and	The evaluator shall provide basis and narrative.
	— (23) ordering of presentations to the PAD enabled and disabled system, and whether *test* subjects were reused.	The evaluator shall provide basis and narrative.

Table 1 *(continued)*

ISO/IEC 30107-3 Clause	Requirement	Approach in Presentation Attack Detection (PAD) testing of mobile devices
13.4.2.1	(24) For a *given verification system IUT*, for each PAI species, *the following shall be reported:* — *IAPAR* and the sample size on which this computed rate is based; *and* — *FS-PD (optional).* *For bona fide test subjects, the evaluator shall report FRR/FAR calculations and the basis of results.* *For a given IUT, the IAPAR of the most successful PAI species with attack potential AP may be reported as* $IAPAR_{AP}$.	The evaluator shall provide results and basis of calculations.
13.4.2.2	(25) *For a given identification system IUT, f*or each PAI species, *the following shall be reported:* — IAPIR and the sample size on which this computed rate is based; *and* — *FS-PD (optional).* *For bona fide test subjects, the evaluator shall report FNIR/FPIR calculations and the basis of results.* *For a given IUT, the IAPAR of the most successful PAI species with attack potential AP may be reported as* $IAPAR_{AP}$.	The evaluator shall provide results and basis of calculations.